Februar 2017. **Broj 46**

LiBRE!

Časopis o slobodnom softveru

Slobodni softver u Bosni i Hercegovini

JOŠ IZDVAJAMO

FAN sistem za nadzor servisa i uređaja

Šifrovanje elektronske pošte na Androidu: K-9 i AGP

Reč urednika

Promene

Velika pauza donosi velike promene. Danas kada se navršava tačno pet godina od ideje za pokretanje časopisa, sa ponosom možemo da vam predstavimo 46. broj Časopisa, uz koji dolaze radikalne promene.

Sa pogledom na prošlost, moramo priznati da je statistika koja se krije iza ovih pet godina zaista zadivljujuća. Preko šezdeset autora je učestvovalo u realizaciji 46 brojeva kao stalni ili povremeni saradnici, a u tim brojevima je obrađeno preko trista različitih tema o slobodnom softveru. Ove činjenice nam nisu dozvolile da odustanemo u momentima kada je dalji nastavak rada Časopisa doveden u pitanje. Probleme kroz koje smo prošli u prethodnoj godini ostavljamo iza sebe, i optimističnim korakom nastavljamo dalje. Ponosni svim dosadašnjim uspesima Časopisa i ohrabreni podrškom naših čitalaca, uveli smo određene promene koje će održati Časopis aktivnim sigurno još pet godina, a nadamo se i više.

Najznačajnija novina je definitivno još jedan oblik LiBRE! časopisa - na dobro poznatoj adresi libre.lugons.org se nalazi LiBRE! blog. „Da li LiBRE! treba da postane blog?” - pitanje je koje se od samog početka Časopisa provlačilo kroz redakciju. Nakon pet godina to se desilo; redakcija je došla do zaključka da je to najefikasniji način da se čitaocima omogući pristup riznici znanja sačuvanoj u prethodnim brojevima. Ovaj potez je povukao sa sobom ostale promene. Ako ste primetili da su vam članci poznati, razlog tome je novi način objavljivanja. Svaki članak pre nego što se pojavi u pdf izdanju Časopisa premijerno će biti objavljen na njegovom sajtu. Postavlja se pitanje čemu onda dalje objavljivanje novih brojeva Časopisa. Nismo želeli da se odreknemo prednosti koje nam takvo izdanje pruža, ali pre svega smo rešili da ostanemo dosledni formi koja nas prati od samog početka i čini jedinstvenim.

Reč urednika

Naredni broj će biti objavljen tek kad se prikupi dovoljan broj tekstova, što će izazvati određene varijacije u periodici izlaženja. Periodika objavljivanja Časopisa zato postaje neodređena, a novi broj će izlaziti kao presek tekstova već objavljenih na sajtu. Posrednički format za mobilne uređaje kakav je ePUB je izgubio svoj smisao, tako da od ovog broja, ePUB izdanje Časopisa više neće postojati.

Takođe, radikalne promene se mogu primetiti u funkcionisanju LiBRE! tima. Oslobađanjem pritiska koje je sa sobom nosila obaveza objavljivanja novog broja jednom mesečno, nadamo se da ćemo privući nove članove u naš tim. Projekat postaje manje zahtevan za sve njegove članove, što pruža mogućnost dužeg rada na člancima, a samim tim i povećanje njihovog kvaliteta.

LiBRE! projekat će ovime dosta usporiti, ali to će mu pružiti mogućnost da se posveti ostalim bitnim segmentima. Pored povećanja kvaliteta tekstova objavljenih u Časopisu, jedna od glavnih težnji biće povećanje uticaja u regionu. LiBRE! kao regionalni projekat će pokušati ubuduće da što više prikaže stanje slobodnog softvera i dešavanja u regionu, što se može već videti u ovom broju člankom koji analizira stanje slobodnog softvera u Bosni i Hercegovini. Nastaviće se sa objavljivanjem starih tekstova; određen deo biblioteke znanja je već dostupan na sajtu, a u narednom periodu možete očekivati postepeno objavljivanje i ostatka tekstova.

Do sledećeg broja,

LiBRE! tim

Sadržaj

Moć slobodnog softvera

Broj: 46

Izvršni urednik: Nikola Todorović

Glavni lektor:
Admir Halilkanović

Lektura:
Jelena Munćan **Saška Spišjak**

Grafička obrada:
Dejan Maglov **Zoran Lazarević**

Dizajn: **White Circle Creative Team**

Autori u ovom broju:
Nikola Todorović **Stefan Nožinić**
Nenad Marjanović **Igor Stoiljković**

Marjan Đuran **Stefan Biševac**
Amar Tufo **Momčilo Medić**
Adrijan Đurin **Petar Simović**

Počasni članovi redakcije:
Željko Popivoda **Mihajlo Bogdanović**
Vladimir Popadić **Željko Šarić**
Aleksandar Stanisavljević

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

E-pošta: libre@lugons.org
Veb: http:/libre.lugons.org

Vesti

9.septembar 2016.

Balkon 2k16

Od 9. do 11. septembra, u Novom Sadu, u kongresnom centru, održao se najveći hakerski kongres na teritoriji Balkana, Balkon 2k16. Četvrti put zaredom, organizatori su uspeli da prevaziđu sami sebe. Za sve koji su propustili ovaj događaj dostupni su snimci sa predavanja.

Korisni link: http://bit.ly/2m0HgAI

13.oktobar 2016.

Ubuntu 16.10

Objavljena je nova verzija popularne Linuks distribucije, Ubuntu 16.10. Najvažnija promena je svakako novi Kernel verzije 4.8, koji donosi veliki broj promena vezanih za stabilnost, brzinu i energetsku efikasnost.

Korisni link: http://bit.ly/2kWcJ5W

---

14. oktobar 2016.

20. rođendan KDE

Zajednica okupljena oko KDE projekta proslavila je svoj dvadeseti rođendan. Zajednica, koja je započeta sa namerom da razvija grafičko okruženje za Linuks operativne sisteme, danas razvija veliki broj korisnih alata, kao i operativni sistem za mobilne telefone.

Korisni link: http://bit.ly/2kMMkXF

---

22. nobembar 2016.

Fedora 25

Fedora operativni sistem je dobila svoje 25. izdanje, koje sadrži veliki broj ispravki.

Korisni link: http://bit.ly/2m0I1tx

24.jul 2016.

Kernel 4.9

Linus Torvalds je objavio kernel 4.9, ovo izdanje ima najviše promena do sada u odnosu na prethodnu verziju; izvršeno je čak 16 hiljada značajnih promena u kodu.

Korisni link: http://bit.ly/2ljKG1H

16. decembar 2016.

Linuks Mint 18.1

Predstavljena je prva ispravka 18. izdanja Linuks Mint operativnog sistema.

Korisni link: http://bit.ly/2kMoLhE

17. decembar 2016.

Lugons BarKamp 5

Na Fakultetu tehničkih nauka u Novom Sadu održan je peti po redu Lugonosov BarKamp, koji se organizovao u saradnji sa Katedrom za Primenjene računarske nauke.

Korisni link: http://bit.ly/2lXF1RL

Vesti

24. decembar 2016.

Linedž OS

Nakon objavljivanja vesti da se projekat Sajnogenmod (eng. *CyanogenMod*) gasi, grupa programera rešila je da nastavi projekat, odvojeno od kompanije Sajnogen I-en-si (eng. *Cyanogen INC*), pod nazivom Linedž OS (eng. *Lineage OS*).

Korisni link: http://bit.ly/2m0D587

23.januar 2017.

Serbian GNU-Linuks 2017

Dostupna je za preuzimanje četvrto izdanje domaćeg operativnog sistema Serbian GNU-Linuks 2017, sa KDE i Openboks grafičkim okruženjem.

Korisni linkovi: http://bit.ly/2kBGMUv
http://bit.ly/2m0BgI7

24.januar 2017.

Vajn 2.0

Popularni program za izvršavanje programa za Vindouz - Vajn (eng. *Wine*) - objavio je novu verziju 2.0, sa podrškom za veliki broj novih aplikacija i igrica.

Korisni link: http://bit.ly/2lwqJ9F

---

1. februar 2017.

Libreofis 5.3

Nedavno je objavljen Libreofis 5.3. Dolazi sa ujednačenom podrškom za prikaz teksta na svim operativnim sistemima, i uz kog je objavljeno i prvo izdanje Libreofis Onlajn (Lool), veb verzije paketa koja se može koristiti u okviru lokalne infrastrukture.

Korisni link: http://bit.ly/2lyTZx6

---

5. februar 2017.

Olimeks Teres I

Iz Bugarske nam stiže potpuno rasklopivi laptop otvorenog hardvera, Olimeks Teres I. Laptop je predstsavljen na Fosdemu u Briselu i može se poručiti.

Korisni linkovi: http://bit.ly/2ljCSwA
http://bit.ly/2lza4Ty

Puls slobode

Deskon 2016

Autor: Nikola Todorović
Fotograf: Vladimir Opsenica

Nakon izuzetno uspešne prve pilot konferencije Deskon 2015, ove godine smo imali priliku da prisustvujemo trodnevnoj hakaton konferenciji Deskon 2016 (http://descon.me/2016/). Kao i prošle godine, Deskon je organizovan u eksperimentalnom umetničkom prostoru ITS-z1 (http://its-z1.org/) umetnika Dragana Ilića, u prigradskom naselju Ritopek, nedaleko od Beograda, a učesnicima konferencije je organizovan poseban prevoz iz beogradskog Haklaba.

Po uzoru na sve veće hakerske konferencije, Deskon je ove godine imao svoj bedž. Međutim, ono što ju je izdvajalo od ostalih jeste prilika da učesnici konferencije svoj bedž naprave sami. Da ne bi došlo do zabune, važno je znati da se pod

bedžom smatra malo parče elektronike. Uz pomoć ekipe iz haklaba koja je osmislila bedž svaki učesnik je uveden u svet elektronike i upoznat sa osnovnim veštinama lemljenja i povezivanje elektronksih komponenti. Nakon dobro obavljenog hardverskog dela, svako je trebao isprogramirati svoj bedž pritom iskoristivši brojne mogućnosti koje nude Arduino moduli, a atelje u kom se dešavao veći deo konferencije dodatno je pospešio kreativnost kod učesnika konferencije.

Konferencija je otvorena uvodnom rečju same organizatorke Željke Desire (Des) Milošević, a ostatak prvog dana je prošao uz međusobno upoznavanje, pripremu za pravljenje bedževa i jedno predavanje. Predavanje je održao Dušan Mihajlović, slušaocima rok muzike osamdesetih poznatiji kao „Dr. Spira", i on je govorio o tome kako usred potrebe da se sve digitalizuje, zbog loše kompresije se gube bitne informacije koje su podaci pre toga sadržavali. Ukazao je na činjenicu da digitalna tehnologija ne može sve da kvantifikuje i prikaže u obliku nula i jedinica.

Drugi dan smo imali priliku da čujemo predavanje Metjua Džeksona, koji je posebno za Deskon doputovao sa Novog Zelanda u Beograd. Metju nam je govorio o svojim projektima kao i o start-apu *Doctor2Go*, čiji je on suosnivač. Nakon Metjua, imali smo priliku da čujemo nešto o domaćem start-apu Stroberi enerdži od strane Kristine Nikolić. Kristina je predstavila njihove proizvode za parkove, koji su poznati kao Stroberi drvo i Stroberi pametna klupa, a ostatak predavanja je protekao u komentarisanju budućih projekata start-apa. Filip Dulić, kreator Deskon bedža, je održao kratko predavanje kao uputstvo za programiranje bedža, nakon čega je softverski izazov mogao da počne.

Puls slobode

Jedna od glavnih atrakcija na imanju umetnika je definitivno bila velika robotska ruka koja je služila umetniku Draganu Iliću kao pomoć i zamena u slikanju. Tokom trajanja konferencije održan je performans koji umetnik planira u narednoj godini da prikaže u muzejima. Performans je nastojao da predstavi i drugu mogućnost robotske ruke, oblika muzičkog instrumenta. Robotska ruka je poput udaraljke pokušala da napravi galamu lupajući po cevima i gvožđu okačenom o zid.

Za vreme cele konferencije bila je aktivna kriptografska zagonetka, koju je sastavio Petar Simović, autor tekstova o kriptografiji i bezbednosti za LiBRE! časopis. Petar je uz pomoć ostalih članova Haklaba održao kripto-parti na kom su svi bili upoznati sa načinom kako da se zaštite od špijuniranja i kako da šifruju svoju komunikaciju putem mejla. Da ni u jednom trenutku ne propadne dobra atmosfera pobrinula su se tri di-džeja, koja su se smenjivala sva tri dana.

Predrag Radović je započeo treći dan sa predavanjem o Etereumu, nakon čega je usledilo predavanje Petra Simovića o blokčeinu (eng. *Blockchain*). Poslednji dan je poslužio za finalizovanje projekata za bedž i njihovo prezentovanje, a žiri je doneo nimalo laku odluku i dodelio nagradu Metju Džeksonu za najbolju upotrebu bedža. Prisustvovali smo jako lepom gestu, jer novčanu nagradu za pobednika hakatona, koju je Metju obezbedio i osvojio, na kraju konferencije je donirao Haklabu. Konferencija je završena opuštenom atmosferom uz razgovore i obećanja da će i sledeće godine svi obavezno doći.

Slobodni softver u Bosni i Hercegovini

Autor: Amar Tufo

Danas, kada slobodan softver nije više što je bio prije dvadesetak godina kada ga je bilo jako teško instalirati i savladati njegove osnovne korake, jer ga je koristila uglavnom određena skupina kompjuterskih entuzijasta - priča je potpuno drugačija i slobodan softver je postao dostupan svima ponudivši nam veliki izvor operativnih sistema koji su namijenjeni kako početnicima, tako i profesionalcima. I, dok u regionu postoje aktivna linuks udruženja koja prenose svoja znanja i iskustva među korisnicima, u ovom članku ćemo pogledati stanje zastupljenosti slobodnog softvera u Bosni i Hercegovini.

Znaju li ljudi uopće šta je linuks?

Zemlje regiona poput Srbije i Hrvatske veoma uspješno prate trendove u svijetu slobodnog softvera. Upravo uspješni portal Linuks Za Sve dolazi iz Hrvatske, a LiBRE! časopis, zasigurno jedan od najboljih časopisa o slobodnom softveru, nastao je u Srbiji. Oni, pored promocije slobodnog softvera, podstiču korisnike da sami zaplove njegovim vodama, jer se veoma često za linuks korisnike kaže da su sami svoji majstori. Bosna i Hercegovina trenutno je zemlja sa najvećim brojem informatički nepismenih ljudi - kako mladih, tako i odraslih. Činjenica je da je informatika danas postala nezaobilazan segment ljudskog života. Svjetska ekonomija počiva na internetu i sličnim tehnološkim novitetima, koji niču svaki dan. Stoga, kada je riječ o našoj zemlji, skoro osamdeset procenata ljudi veoma slabo koristi ili poznaje računare i njihovu terminologiju. Tako je slobodan softver samo jedno od „španskih sela”. Smatramo da takvom stanju našeg društva uglavnom doprinosi školski obrazovni sistem, ali i veoma loše glasine o linuks operativnim sistemima: naprimjer, da su komplikovani; da su namijenjeni samo hakerima, programerima; da nema podrške drajvera, i slično. S druge strane, ključnu ulogu „udaljavanja” od istih pospješuju tehnički fakulteti te prodavnice

kompjuterske tehnike. Nije sve ni tako crno, pa u ovoj našoj zemlji možete pronaći i velik broj informatičkih entuzijasta koji spadaju među napredne korisnike računala, koji programiraju, i koji ne koriste računala samo za razonodu. Tako se i sami iznenadimo kada susretnemo ljude koji poznaju linuks, koji ga dugo koriste i koji znaju njegove prednosti u odnosu na konkurenciju. Morali bismo ovdje biti iskreni i reći da broj tih ljudi nije tako veliki, ali je pohvalan. O tome koliko je populacija u Bosni i Hercegovini informatički (ne)pismena pročitajte na linku (http://ceppei.ba/bos/index.php?option=com_content&view=article&id=4874&Itemid=72)

Udruženja Linuks korisnika

U regionu djeluju aktivno linuks udruženja koja nesebično šire i prenose znanje na druge; održavaju razne edukacije, seminare, druženja i to sve u cilju poboljšanja informatičkog obrazovanja. Među njima možemo pomenuti LUGoNS (Srbija), HULK (Hrvatska), Ubuntu Srbija, Ubuntu Hrvatska, već pomenuti portal Linuks Za Sve, kao i LiBRE! časopis. Kakva je situacija u Bosni i Hercegovini? Linuks udruženja u BiH nema mnogo, barem ne onih koji su tako aktivna. Međutim, malo boljim pretraživanjem pronaći ćete „Udruženje Linux korisnika BiH" (http://www.linux.org.ba/), koje je osnovano 1998. godine. Udruženje je aktivno promovisalo upotrebu linuksa, te održavalo i edukacije u oblasti linuksa na Elektrotehničkom fakultetu u Sarajevu. Udruženje nije aktivno posljednje četiri

godine zbog nepoznatih razloga. Također, treba pomenuti ULKRS (http://ulk.rs.ba/). Za one koji ne znaju, riječ je o Udruženju GNU-Linuks korisnika Republike Srpske, koje je osnovano 27. januara 2010. godine, a koje, nažalost, također nije više aktivno. Kada je riječ o drugim udruženjima, ovdje možemo pomenuti ona koja djeluju i postoje isključivo na društvenim mrežama, a koja okupljaju veliki broj linuks korisnika i daleko su aktivniji. To su: Ubuntu Udruga BiH, Implementacija Linuks OS u Bosni i Hercegovini te Ubuntu linuks grupa Bosne i Hercegovine (eng. *The Linux OS Ubuntu group Bosnia and Herzegovina*). Ova tri udruženja, koja uglavnom djeluju na Fejsbuku, vrijedno promovišu upotrebu linuksa i slobodnog softvera u svakodnevnom životu, a okupljaju blizu pet stotina aktivnih članova, što je jako pohvalno. Ovdje bismo još samo dodali linkove za prva dva navedena udruženja:

Publikacije i projekti o linuksu

Kod nas trenutno ne postoji nijedan nama poznat magazin koji piše isključivo o slobodnom softveru. Međutim, tu su neki drugi internetski portali kao što je INFO Online i Tehnografija koji među standardnim temama iz svijeta IT noviteta pišu usput i o novitetima u linuks svijetu. Od projekata svakako možemo pomenuti BHLD (eng. *Bosnian Linux Distro*), prvu Bosansku linuks distribuciju koja je razvijena još 2004. godine na Elektrotehničkom fakultetu u Sarajevu. Projekat je imao nekoliko uspješnih izdanja, ali je iznenada prekinut još 2011. godine. Među

drugim projektima koje možemo pomenuti je i DebKonf11, Debijanov događaj koji je bio održan u Banjoj Luci od 24. do 30. jula 2011. godine. Veoma vrijedan pomena je i BarKamp, koji se održava na Elektrotehničkom fakultetu u Banjoj Luci i koji već četvrti put za dvije godine okuplja velik broj stručnjaka sa zanimljivim predavanjima. Izveštaj sa drugog BarKampa je moguće pročitati u četrdesetom broju časopisa ili na sajtu (https://libre.lugons.org/index.php/2015/11/izvestaj-sa-barkamp-konferencije-iz-banjaluke/).

Mogla bi se još pomenuti i modifikovana linuks distribucija za veb dizajn po imenu Slobeliks 12 Veb Dizajn, projekat trojice studenata sa Fakulteta za informacione tehnologije Univerziteta u Bijeljini. Kako se navodi u zvaničnom članku o ovom interesantnom projektu, Slobeliks je namijenjen isključivo za veb dizajn, opremljen velikim brojem alata otvorenog koda kao što je Aptana Studio,

te Blufiš - namjenjenim veb programerima i dizajnerima.

Zaključak

Slobodan softver u Bosni ima velike potencijale ukoliko se razvije adekvatna obrazovna strategija koja bi isključila informatičku edukaciju mladih na računarima sa komercijalnim softverom, a više u fokus stavila obuku korištenja linuks distribucija i Libre Ofisa koji predstavlja sjajan ofis-paket i trenutno najbolju besplatnu alternativu komercijalnom Majkrosoft Ofisu. Naš obrazovni sistem je takav da se linuks operativni sistemi rijetko kada mogu vidjeti u stalnim obrazovnim programima kako naših škola, tako i tehničkih fakulteta. Takvo stanje linuks operativnog sistema na terenu se pravda time što je Vindouz dominantna platforma, a više od 80 procenata računala u Bosni i Hercegovini ih koristi što u javnom, tako i u privatnom sektoru - dok je linuks ostavljen po strani. Fakulteti i škole jednostavno ne pružaju obuku korištenja linuks operativnih sistema, niti podstiču svoje studente i učenike na korištenje slobodnog softvera. Srećom, postoje ljudi, studenti i entuzijasti u ovoj zemlji koji vide veliku prednost slobodnog softvera te sami stiču vještine u korištenju, edukaciji i promociji linuksa i filozofije slobodnog softvera.

fedora 24

Autor: Momčilo Medić

Poslednje izdanje GNU/Linuks distribucije Fedora donosi umeren broj promena. Naime, većina unapređenja se odnosi na izmene unutar sistema, dok je broj vizuelnih razlika prilično mali.

Gnom je u verziji 3.20 i poklapa se sa uzvodnim izdanjem, a dolazi sa novim prikazom tastaturnih prečica, unapređenom pretragom datoteka, kontrolom medija u „kalendarskom meniju" kao i poboljšanim podešavanjima za poslove štampe i upravljanje mišem. Novina, koja je kroz nadogradnje takođe stigla i u prethodnu verziju (23), jeste i to da su sistemske nadogradnje na poslednje izdanje Fedore moguće i kroz grafički interfejs. Aplikacija Softver će u pozadini

preuzeti potrebne datoteke i ponuditi vam ponovno pokretanje sistema sa nadogradnjom. Po običaju mešanje programa koji ne dolaze uz distribuciju mogu uzrokovati neočekivane posledice. U tom slučaju obratite dodatnu pažnju. U istom programu je uvedena i podrška za Flatpakove, novi sistem distribucije softvera koji bi trebalo da obezbedi potpuno izolovano instaliranje i pokretanje programa.

Libre ofis koji stiže uz ovo izdanje Fedore je verzije 5.1 i sa sobom donosi brojna poboljšanja u rukovanju Gnumerik, Mikrosoft.vri i Epl Kinot dokumentima, kao i izvozu u *OOXML*, MS Visio i Korel drou formatima. Promena na GTK+ 3 će učiniti da Libre ofis izgleda još više kao deo sistema, a podrška za Vayland je sada potpuno prirodna i spremna je za korisnike koji su već prešli na novi grafički server. Kada smo već pomenuli Vayland, potrebno je dodati da je sada spreman za svakodnevnu upotrebu i da se očekuje da će biti podrazumevani grafički server od sledeće verzije Fedore.

Serverska edicija Fedore ima novu šemu particionisanja i sada nije neophodno „zauzeti" sav prostor na disku nego se to može i naknadno uraditi čak i pomoću grafičkog veb-alata Kokpit. Ostale izmene obuhvataju smanjenje zauzetog prostora pri instalaciji izuzimanjem određenih paketa, kao i FreeIPA domenski kontroler u verziji 4.3.

U nastojanju da Fedora klaud postane najbolja platforma za kontejnere, od sada je u distribuciji dostupan i Openšift origin, sistem zasnovan na Kubernetes koji služi za orkestraciju kontejnera.

Izvedbe Fedore prate novo izdanje i pružaju skup programa i alata koji treba da zadovolje specifične namene. Ako ne želite da koristite podrazumevano Gnom okruženje i isprobate nešto drugačiji izgled, a pritom i dalje koristite poznate alatke za upravljanje sistemom, onda su za vas dostupne izvedbe kao što su KDE, Iks-ef-se-i (eng. *Xfce*), Sinamon, ... Takođe postoje i izvedbe organizovane oko specifičnih namena kao što su muzičko stvaralaštvo, robotika, igranje, sigurnost, naučni rad i slično.

Većina prosečnih korisnika neće primetiti razliku između prethodne i aktuelne verzije Fedore, ali to pokazuje da izmene koje se uvode nisu radikalne i ne prouzrokuju uzurpaciju načina rada na koji ste navilki. Takođe, zajednica nikako nije dokona i konstantno radi na usavršavanju sistema, unapređenju stabilnosti kao i poboljšanju samih alata kojim se održavaju infrastruktura i pravi sama Fedora.

Fedora Srbija zajednica vas podseća da ste svi dobro došli i cenjeni kao saradnici. Bez obzira na vašu stručnost, profesiju, zanimanje ili slobodno vreme, svako od vas može da učini Projekat boljim za sve.

Kako da...?

Numerička obrada i simulacije

(7. deo)

Autor: Stefan Nožinić

Kako se opisuju fizički sistemi

Svaki fizički sistem ima neki model koji ga opisuje ili aproksimira. Najjednostavniji primer je padanje loptice na pod. Mi znamo da na lopticu deluje gravitaciona sila i na osnovu toga primenjujemo drugi Njutnov zakon. Za datu lopticu imamo jednačinu koja nam opisuje koliko u datom trenutku iznosi ubrzanje loptice. Kako naša loptica ima isto ubrzanje u svakom trenutku - gravitaciona sila se ne menja, što znači da se njena brzina menja linearno (povećava se) a da se pređeni put može opisati kvadratnom funkcijom. Kako ovo znamo? Ubrzanje je promena brzine u jedinici vremena (izvod brzine), a brzina je promena pređenog puta u jedinici vremena, odnosno ubrzanje je drugi izvod pređenog puta. Kako naš model iskazuje koliko je ubrzanje loptice, mi moramo da to ubrzanje integralimo dva puta kako bismo dobili pređeni put. Jednačina koja opisuje kretanje loptice je diferencijalna jednačina.

Zapravo, svaki fizički sistem se može opisati kao diferencijalna jednačina.

Diferencijalne jednačine prvog reda

Ovaj tip je osnovni tip diferencijalne jednačine. Za datu funkciju x (koja može biti pozicija ili nešto drugo) diferencijalna jednačina je:

$$\frac{dx}{dt} = f(t, x)$$

Sa leve strane nam se nalazi promena funkcije u zavisnosti od promene vremena, a sa desne strane nam se nalazi vrednost te promene.

Ojlerov metod za rešavanje diferencijalne jednačine prvog reda

Najjednostavniji način da rešimo gore opisani tip jednačine je sledeći:

Ako imamo vrednost naše funkcije u nekom trenutku i ona iznosi $x(t)$, mi želimo da odredimo narednu vrednost funkcije. Kako su računari diskretne mašine i ne možemo previše ići u detalje - ne možemo odrediti vrednost funkcije baš u svakom trenutku. Ono šta možemo uraditi jeste da izračunamo u približnom trenutku posle Δt vremena odnosno da odredimo

$$x(t + \Delta t)$$

Ovo možemo uraditi baš zahvaljujući postavci naše jednačine jer je:

$$\frac{x(t + \Delta t) - x(t)}{\Delta t} = f(t, x)$$

Kada ovo sredimo, imamo Ojlerov korak za naredni vremenski korak:

$$x(t + \Delta t) = x(t) + \Delta t f(t, x)$$

Diferencijalne jednačine drugog reda

Ovo su složenije jednačine, ali se vrlo lako prebacuju na jednačine prvog reda. One su oblika:

$$\frac{d^2x}{dt^2} = f(t, x, \frac{dx}{dt})$$

odnosno, može se i lakše zapisati kao $x = f(t,x,x')$ Ako bi nam x bio pređeni put onda je x' brzina a x'' nam je ubrzanje.

Kako ovo rešavamo? Uvedemo smenu $v = x'$ i onda imamo sledeću situaciju: $v' = f(t,x,v)$ i $x' = v$

Prvo rešimo prvu jednačinu pomoću Ojlerovog metoda, a onda novu vrednost za brzinu ubacimo u drugu:

$$v(t + \Delta t) = v(t) + \Delta t f(t, x, v)$$
$$x(t + \Delta t) = x(t) + \Delta t v(t + \Delta t)$$

Kako da...?

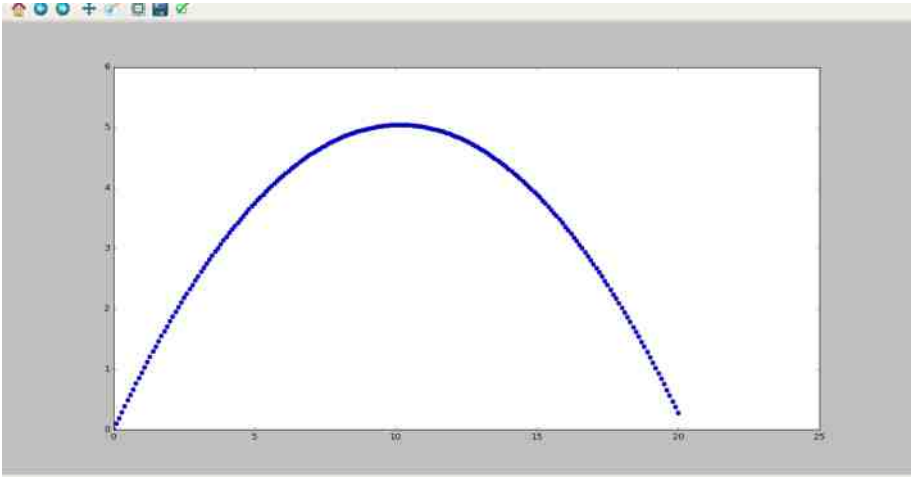
Primer - kosi hitac

Evo i primera kako bismo uradili simulaciju bacanja loptice ukoso.

```
import numpy as np
import matplotlib.pyplot as plt

# Prvo zadajemo pocetne vrednosti, imamo dve koordinate, radimo sa
dve pozicije i dve brzine
# jedna za  a druga za y koordinatu loptice

x = 0.0
y = 0.0

v_x = 10
v_y = 10

dt = 0.01 # vremenski pomeraj

def f_y(t, x, v):
    return -9.81 # ubrzanje po y-osi na dole

def f_x(t, x, v):
    return 0 # ubrzanje po x-osi

p_x = [x] # ovde čuvamo x vrednosti da plotujemo
p_y = [y] # ovde cuvamo y vrednosti da plotujemo

# uradimo nekoliko iteracija i dodajemo nove vrednosti u niz za
plotovanje
for i in range(200):
    t = i * dt
    v_x = v_x + dt * f_x(t,x,v_x)
    x = x + dt*v_x

    v_y = v_y + dt * f_y(t,y,v_y)
    y = y + dt * v_y
    print(x)
```

```
    print(y)
    print()
    p_x.append(x)
    p_y.append(y)

plt.plot(p_x, p_y,  "o")
plt.show()
```

Potrebno je primetiti da ovde imamo dve pozicije, dve koordinate pošto radimo u dvodimenzionalnom sistemu. Kod možemo i kraće napisati ako definišemo poziciju i brzinu kao vektore.




```
import numpy as np
import matplotlib.pyplot as plt

# Prvo zadajemo pocetne vrednosti, imamo dve koordinate, radimo sa
dve pozicije i dve brzine
# jedna za  a druga za y koordinatu loptice
```

```
x = np.array([0,0])

v = np.array([10, 10])

dt = 0.01 # vremenski pomeraj

def f(t, x, v):
    return np.array([0, -9.81]) # ubrzanje

p_x = [x[0]]
p_y = [x[1]]

# uradimo nekoliko iteracija i dodajemo nove vrednosti u niz za
plotovanje
for i in range(200):
    t = i * dt
    v = v + dt * f(t,x,v)
    x = x + dt * v

    p_x.append(x[0])
    p_y.append(x[1])

plt.plot(p_x, p_y,  "o")
plt.show()
```

Dodatni metodi za numeričko rešavanje diferencijalnih jednačina

Često Ojlerov metod nije dovoljno stabilan ili tačan. Zbog ovoga postoje i druge metode kao što su Runga-Kuta i implicitni metodi. Predlažemo vam da pronađete na internetu kako se oni koriste kako ne biste dolazili do problema da vam Ojler ne rešava problem dovoljno stabilno ili tačno.

KiPasIks

Autor: Marjan Đuran

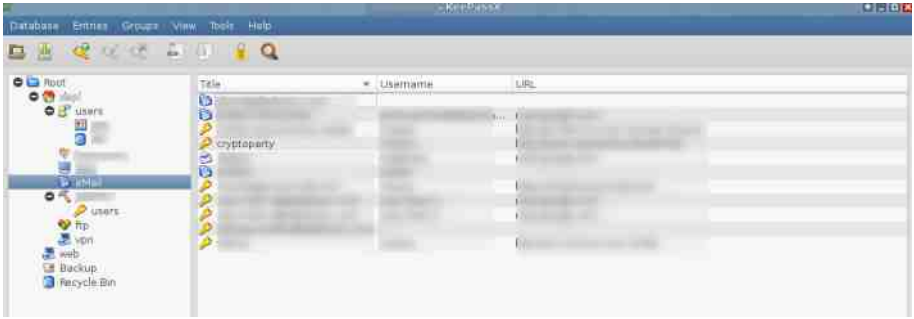
Zašto

Jedan od vidova bezbednosti jeste šifra. Danas prosečan korisnik ima minimalno pet različitih naloga: za mejl, omiljeni forum, društvenu mrežu, onlajn prodavnicu i ko zna šta još, a sve od navedenog može biti i u množini. Jedini način na koji korisnik može da utiče na bezbednost svog naloga jeste da ima „dobru" šifru (i da je redovno menja). Šta znači dobra šifra? Više o šiframa mogli ste čuti i na Balkonu (eng. *Balccon*) 2015. godine (http://goo.gl/6PRv4H). Ukratko, šifra ne sme biti ništa smisleno. Najjednostavnije rečeno, trebalo bi da je nasumično generisan, što duži niz što različitijih karaktera. Tu se javlja nekoliko problema, prvi je kako generisati? To je zapravo najmanji problem i može se rešiti na više načina. Možemo da iskuckamo žmureći nasumično po tastaturi, generisati heš (eng. *hash*) bilo čega, koristiti *rand()* funkcije ili programe za to namenjene. Ali problem kako tako nasumično generisanu šifru upamtiti, a kako tek pet ili više njih (dobro je poznato pravilo da se šifre ne smeju zapisivati po ceduljicama), ne može baš bilo koja aplikacija da reši. KiPas je jedna od retkih aplikacija koja može da se pohvali gotovo svim segmentima manipulisanja i vladanja šiframa.

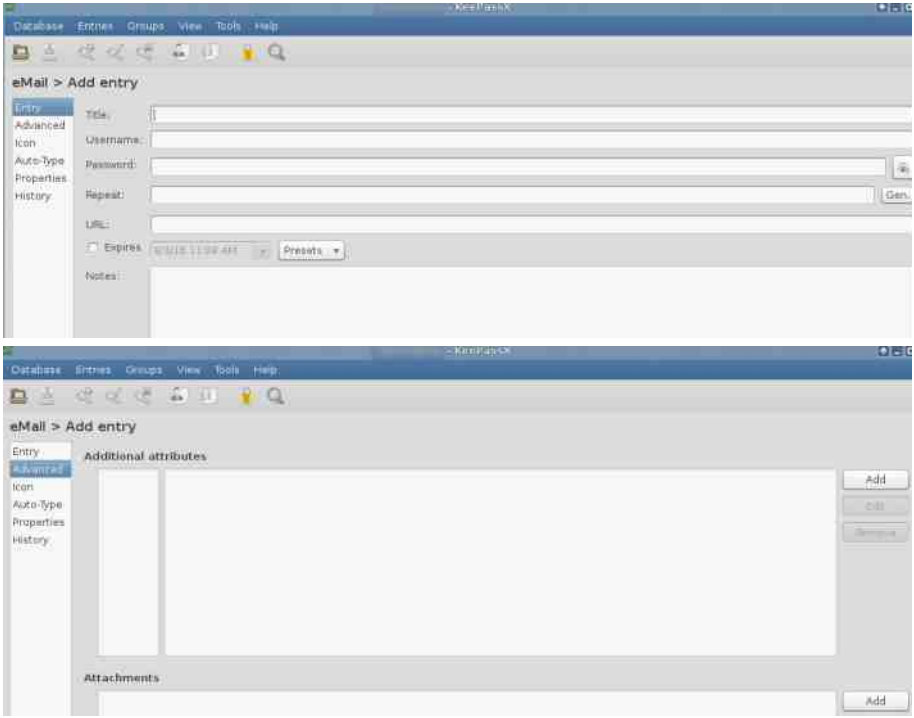
Šta je i kratak opis

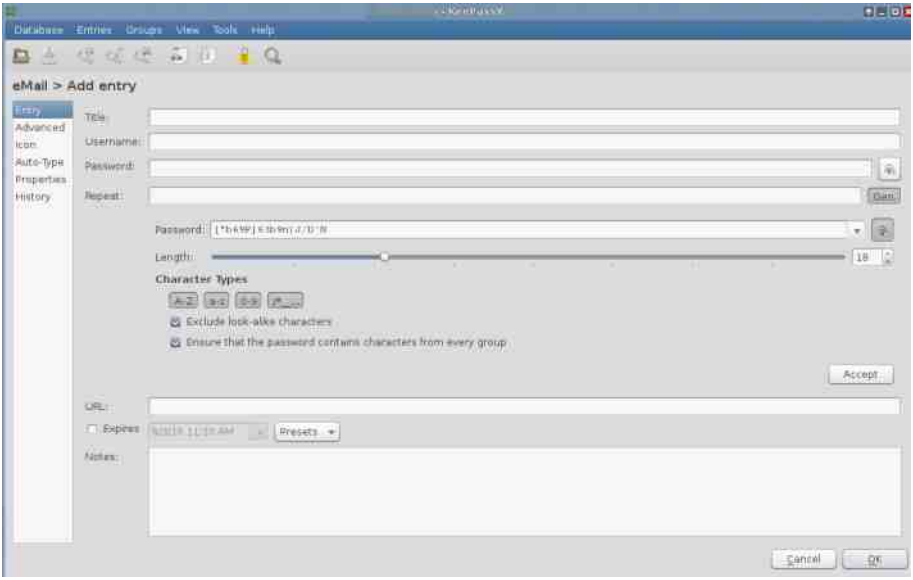
KiPas je aplikacija koja služi za čuvanje šifara, pored toga ima mogućnost i generisanja šifara uz odabir karaktera koji će učestvovati i njihovog broja, sve to uz prilično lepo organizovan grafički interfejs koji je vrlo jasan i pregledan. U levom delu nalaze se grupe i podgrupe koje možete sami kreirati organizovati, npr. mejl, društvene mreže, forumi... Dok se sa desne strane otvara spisak kredencijala za odabranu grupu ili mogućnost za novi unos.

Kako da...?



Sve što u programu želite da uradite, možete na više načina, kroz tulbar (eng. *toolbar*), desnim klikom ili skraćenim putem, kombinacijom tastera na tastaturi. Dodatna mogućnost jeste da se uz svaki unos šifre, pod opcijom „*Advanced*" doda i neki atribut npr. kratak opis koji sadrži određeni tekst ili čak prilog (eng. *attachment*), koji će takođe biti šifrovani.





Još jedna od pogodnosti je što KiPas možete, ali ne morate instalirati. Dakle, možete da nosite sve svoje kredencijale šifrovane na USB fleš memoriji. Postoji i mogućnost višekorisničke upotrebe. U praksi to znači da bazu možete držati na deljenom ili mrežnom disku, i da njoj može pristupati više ljudi. Postoji i mogućnost uvoženja iz datoteka *XML*, *CSV*, *TXT* ekstenzija.

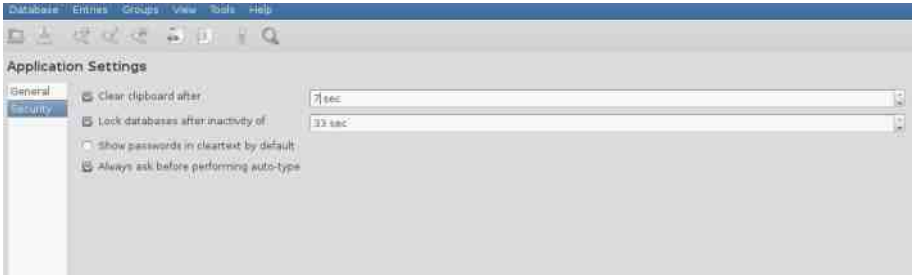
Šta to izdvaja KiPas? Pored jednostavnosti korisničkog dela, KiPas izdvaja to što sve šifre čuva u internoj bazi (koju korisnik vidi kao običnu datoteku) koja je šifrovana kombinacijom dva algoritma - AES i Tufiš (eng. *Twofish*). Na zvaničnom sajtu se posebno napominje da nisu samo polja sa šiframa enkriptovana, već cela baza.

Malo kriptografije

Kratak opis algoritama koji se koriste. AES (eng. *Advanced Ecryption Standard*) simetrični algoritam koji zadovoljava sigurnosne zahteve u većini primena, do sada nisu pronađeni nesigurni ili potencijalno nesigurni ključevi. Temelji se na Rijdil (eng. *RIJNDAEL*) algoritmu koji je otporan na linearne i diferencijalne kriptoanalize. Razvili su ga Joan Daemen i Vinsent Rijmen. Tufiš (eng Twofish) je tzv. AES finalista, simetričan blokovski algoritam koji prema autorima nema

slabih ključeva, ali ima jednostavan dizajn koji olakšava analizu i implementaciju. Razvijen je od strane kompanije Kanterpejn sistems (eng. *Counterpane Systems*), a autori su Brus Šnajer, Džon Kelsej, Dag Vajting, David Vagner, Kris Hal i Nils Ferguson. Oba algoritma šifruju blokove teksta 128 bita, ključem dužine 256 bita.

Pored toga, glavna šifra (eng. *master password*) se čuva u obliku SHA256 heš (eng. *hash*) funkcije. Šta to znači? Heš funkcija oblika je $y=f(x)$, za neku datoteku bilo koje veličine ili tekst bilo koje dužine karaktera (x) dobićemo heš funkciju (y) uvek iste dužine. Na primer, ako je prethodna rečenica ulaz, izlaz izgleda ovako: **6205f2515ec0f62920d33759d31ee37eb5aa8d5da6b0370915b72349dfaa039a**. Jedna od mnogobrojnih primena heš funkcija jeste čuvanje šifara na disku, pa se tako i ovde koristi. Izabrana je heš funkcija SHA256(eng. *Secure Hash Algorithm 256*), 256 je dužina dobijene funkcije, razvijena je od strane NIST-a i NSA agencija. Primer SHA256 algoritma http://goo.gl/piuL0k. Da se vratimo samoj aplikaciji, jedna od takođe zanimljivih mogućnosti jeste da za bazu ne koristitie šifru, već ključ (eng. *key file*). Iako na prvi pogled zvuči kao neki ključ koji je potrebno generisati kao za SSH, u pitanju je zapravo bilo koja datoteka. Dakle, možete koristiti film, tekst, sliku... Ova opcija je naročito korisna ukoliko strahujete od kilogera (eng. *key logger*), ali se može koristiti i u kombinaciji sa šifrom i time povećati nivo sigurnosti vaših šifara. Takođe postoji i memorijska (eng. *In-Memory Streams*) zaštita, što znači da se koristi ključ sesije (eng. session key) dok se učitava program u memoriju i da su šifre čak i tada bezbedne, kao i zaštita od napada grubom silom (eng. *bruteforce attack*).



Kroz tulbar meni, u „*application settings*" meniju, može se podesiti vreme čišćenja klipborda, odnosno, nakon koliko vremena će se šifra ili korisničko ime koje ste kopirali iz KiPas-a, obrisati i postati nedostupna za ponovno nalepljivanje

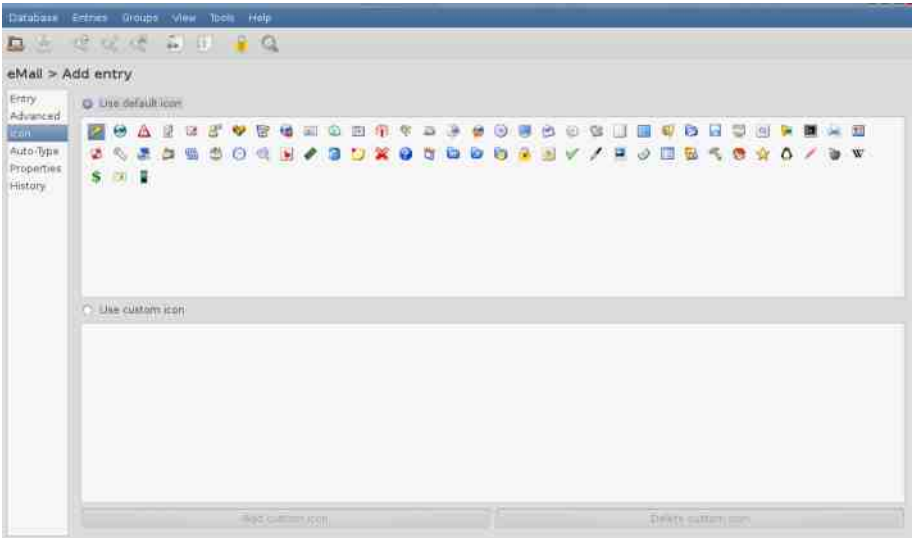
tj. pejstovanje (eng. *paste*). Takođe, može se podesiti i vreme samozaključavanja baze nakon određenog vremena neaktivnosti, u slučaju da odete od računara, a ostavite bazu otključanu.

Pluginovi

Postoji dosta pluginova za KiPas, sve ih možete naći na http://goo.gl/jdOkm6, ali ovde su izdvojena samo tri.

1. KiPasRFID - dodatak koji omogućava dešifrovanje baze pomoću RFID ili NFC čipa posredstvom potrebnog hardvera, može biti odličan dodatak bezbednost vaše baze.
2. *QR* Kod Generator - omogućava prikaz šifre u obliku QR koda, zanimljiv način čuvanja šifre, zamislite da nosite nalepnicu sa QR kodom na telefonu, skenerom na vašem računaru otključavate KiPas bazu!
3. *Application Icons* - KiPas ima svoj set ikonica, iako je moguće da sami uvezete bilo koju drugu (budite oprezni sa uviženjem ikonica preuzetih sa interneta, prethodno ih proverite), ovaj plugin ima svoj set novih ikonica.

Kako?



Kako da...?

Kipasiks se nalazi na repozitorijumima gotovo svih distribucija, i možete ga instalirati jednom komandom.

Fedora:

```
dnf install keepassx
```

Centos:

```
yum install keepassx
```

Arč:

```
pacman -S kepassx
```

Debian i derivati (Ubuntu, Mint, Kali):

```
apt-get install keepassx
```

Na posletku, KiPas je (podrazumevano) besplatna aplikacija otvorenog koda, dostupna je za gotovo sve platforme: linuks, Vindouz, OS Iks, Android, Vindouz Fon, Ajfon, Hrombuk, BlekBeri, čak i za java mobilne platforme (*J2ME*), Palm OS, za veb-pretraživače postoji KiVeb, a za potrebe onih koji ne vole grafičko okruženje ili su iz nekog razloga sprečeni da koriste GUI, tu je KPCLI o kojem će biti reči u nekom od narednih tekstova.

Za sada, KiPas ima sam jednu konkurentsku aplikaciju, zove se Gorila menadžer šifara, takođe je otvorenog koda, takođe koristi SHA256 algoritam za heširanje glavne šifre (eng. *master password*), takođe koristi Tufiš (eng. *Twofish*) algoritam za šifrovanje baze (ali samo njega), i svojim grafičkom interfejsom dosta liči na KiPas. Više o Gorila aplikaciji možete videti na http://goo.gl/1436mh, a ovde u nekom od narednih tekstova.

Kako do sigurnijih šifara?

Autor: Petar Simović

Kada pomislimo o privatnosti naših podataka, prvo što nam padne na pamet trebalo bi da je šifra. Zašto? Zato što se u suštini klasično simetrično šifrovanje svodi na šifru koju korisnik unese i podatak na koji se ta šifra primenjuje upotrebom određenog algoritma konačan broj puta. Pogledajmo gde se zapravo danas sve oslanjamo na šifre kako bismo se zaštitili od napadača i očuvali privatnost. Najpre, svi koristimo imejl, onda društvene mreže poput Fejsbuka i Tvitera, zatim, možda smo aktivni i na forumima ili koristimo neku od klaud usluga čuvanja podataka, tu je i pristup našem računaru ili telefonu, bežična (eng. *Wi-fi*) mreža na koju smo povezani, i tako dalje. Lista može biti opterećujuće dugačka, i morate voditi računa o svim tim šiframa za pristup određenom nalogu.

Situacija u kojoj prosečan korisnik ima više od desetak naloga za koje treba da pamti šifre svakako predstavlja problem i vodi ka korišćenju jedne šifre za sve naloge, ili upotrebi veoma kratkih i jednostavnih šifara. Štaviše, korisnici su često skloni zapisivanju šifara u jednoj nezaštićenoj tekstualnoj datoteci koju, da stvar bude gora, čuvaju na nekom USB-u koji dalje priključuju na druge neproverene računare. Čest je i slučaj da se šifre između korisnika razmenjuju putem nezaštićenih komunikacija kao što su imejlovi, sms poruke, tviter ili fejsbuk direktne poruke, pa i slanjem u obliku tekstualne, ljudski čitljive, datoteke. Neretke su i situacije u kojima administratori ili dizajneri nekog mrežnog servisa ili platforme pogrešno rukuju korisničkim šiframa iz neznanja, nedostatka novca ili vremena. Tako je čest slučaj da se šifre korisnika na nekom sajtu čuvaju u tekstualnoj i ljudski čitljivoj datoteci tzv. pleintekstu (eng. *plain text*) ili nezaštićenoj bazi podataka, ili se slanje šifre između korisnika i servera ne obavlja preko zaštićene veze tj. ne koristi se SSL.

Kako da...?

Šta je sigurna šifra?

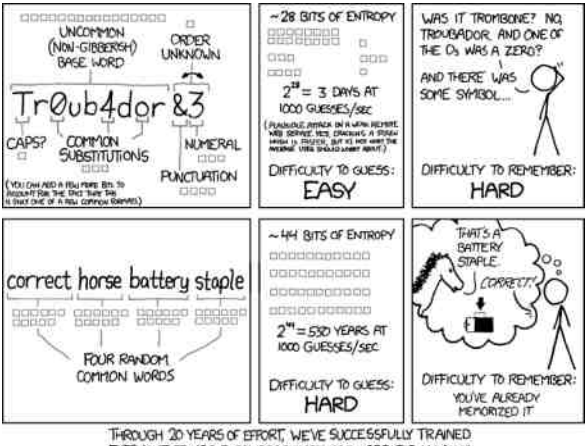
Kako bismo odgovorili na ovo pitanje, moramo prvo znati kako se meri sigurnost šifre, tj. moramo uvesti pojam **entropije**. Entropija je broj bitova koji izražava koliko je šifra jaka poredeći je sa odgovarajućim nizom nasumičnih bitova. Tačna formula je jednostavna i ako entropiju obeležimo sa *E* uključuje dužinu šifre *D* i skup/set mogućih karaktera iz koga je šifra odabrana *S*: $E = \log_2(S^D)$.

Primera radi, ako koristimo samo slova iz azbuke (*S=30*) za sastavljanje naše šifre, i ako nam je šifra dužine 8 slova/karaktera (*D=8*), entropija će biti 39,25 ($\log_2(30^8)$ https://goo.gl/vcAvO) ili oko 4.9 bita entropije po slovu (ako se koriste samo mala ili samo velika slova). Naravno entropija od 39,25 bita nije dovoljna da zaštiti važne tajne. Preporuka je da u zavisnosti od vrste napada koju napadač izvodi, entropija bude veća (**80+ bitova**) za oflajn napade i (**40+ bitova**) za mrežne napade. Razlika je u tome što ukoliko napadač ne može da dođe u posed šifrovanim datotekama ili heširanoj šifri, moraće da pokušava da pogodi vašu šifru direkno na mreži servisa što je sporije i što se lakše uočava i sprečava. Međutim, entropija nije najbolja mera, jer **kompleksnost** šifre nije uračunata. Tako, na primer, naša šifra od 8 karaktera mogla je biti „lubenica" koja nije kompleksna iako ima sva različita slova. Stvar je u tome da je „lubenica" reč iz rečnika i to je čini neotpornom na napade rečnicima (eng. *dictionary attack*). Tu dolazimo do još jednog važnog aspekta kada je u pitanju način na koji korisnici sastavljaju svoje šifre, a to je **nasumičnost**. Šifra „lubenica" nije spoj nasumično odabranih slova azbuke, već ciljano birana reč. Razna istraživanja pokazuju da su ljudi veoma loši u sastavljanju nasumičnih šifara jer sve rade po nekoj logici ili obrascu. Ni računari nisu savršeni izvor nasumičnosti, ali sa ovog aspekta su bolji od ljudi. Zato je važno napomenuti da je entropija dobar pokazatelj sigurnosti šifre ako se karakteri biraju nasumično, a ne ciljano. Ako koristite engleski alfabet prisutan na tastaturama, pored slova koristite i brojeve i specijalne karaktere „**012345678**9" (10 karaktera) „**~`!@#$%^&*()_+-={}|[]\/;':"/.,?><**" (33 karaktera) tj. sve Aski (eng. *ASCII*) karaktere koji se mogu odštampati. To je ukupno 95 karaktera (26 malih slova, 26 velikih, 33 specijalna karaktera i 10 brojeva). Skup od 95 karaktera vam daje i veću entropiju po karakteru, tj. imate oko 6.5 bita entropije po karakteru iz ovog skupa.

Pored šifara postoje i **fraze** (eng. *passphrase*) koje u ovom kontekstu označavaju reči iz rečnika. Naime, umesto da koristimo skup slova iz abuke ili abecede, koristićemo rečnik kao skup poznatih reči. Sigurno se pitate „Reči iz rečnika? A

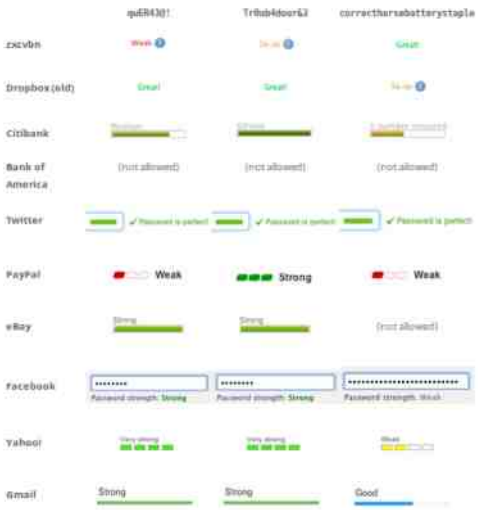
šta je sa napadima rečnika". Odgovor je zapravo jednostavan. Rečnik ima mnogo veći skup elemenata tj. reči nego što azbuka ima slova, pa je odabir par reči bolji od odabira nekoliko karaktera. Ovaj koncept se zasniva na tome da je lakše upamtiti 4 nepovezane i nasumično izabrane reči iz skupa od 7776 reči nego 8 nasumičnih karaktera iz skupa od 95 ($\mathbf{\log_2(7776^4) = 51; \log_2(95^8) = 52}$) za istu entropiju sigurne šifre.

Istaknimo još jednom da je nasumičnost važno svojstvo procesa generisanja sigurnih šifara ili fraza. Entropija kao mera sigurnosti šifre ili fraze je tačnija ako se šifra sastavlja od nasumično biranih karaktera, odnosno fraza od nasumično biranih reči iz određenog skupa. Međutim, nasumičnost je još važnija za odbranu od napada **socijalnim inženjerigom** (eng. *Social Engineering*) o kome ste mogli da pročitate u 39. broju. Kako biste izbegli da napadač poznajući vas, vaše navike i interesovanja može lako da pogodi vašu šifru, najbolji način je da izbor šifre ili fraze prepustite nasumičnosti. Sastavljanje sigurne fraze može biti i zanimljivo ili čak ličiti na dečju igru jednostavnom **dajsver** (eng. *Diceware* https://goo.gl/oukz5n) metodom. Uzmite listu reči ili rečnik (možete naći i preuzeti sa https://goo.gl/pXBYJL ili https://goo.gl/AABLJE) i jednu kockicu. Zatim bacite pet puta kockicu i zapišite brojeve koje dobitete (na primer ako dobijete 32512 taj broj će odgovarati reči „heat" u listi https://goo.gl/ZUOLQW na strani 14.) Znači pet bacanja kockice vam daje jednu reč, a treba vam najmanje 4 reči za sigurnost fraze od preko 50 bitova entropije.



Kako da...?

Važna napomena je i da zamenjivanje slova „A" sa brojem „4" ili karakterom „@", ili slovo „O" sa brojem „0" ili karakterom „*" neće unaprediti sigurnost šifre, već će vam samo dati lažan osećaj sigurnosti. Kada napadač pokuša da probije neku šifru, on naravno zna za zamene ove vrste i napraviće program koji će reči iz rečnika probati i zamenom određenih karaktera za brojeve. Na primer šifra *„MyPassword123"* sa zamenama može da izgleda *„MyP@SSw0rd123"*. Da stvari budu gore, po neiskusne korisnike, kada ovakvu šifru za zamenjenim karakterima isprobate u nekim od poznatih onlajn merača sigurnih šifara, dobićete zadovoljavajuće ili čak odlične ocene jačine vaše šifre (rezultate možete videti na: http://imgur.com/a/mjV4I). Dok za istu šifru, drugi merači sigurnosti šifara daju realnije rezultate (rezulate možete videti na: http://imgur.com/a/Yla5t). Nisu svi merači sigurnosti šifara isti.



Kada smo već kod onlajn merača sigurnosti šifre, budite veoma oprezni. Iako većina tvrdi da ne prikupljaju vaše šifre koje proveravate na tim sajtovima, takvu tvrdnju je teško proveriti. Zato savetujemo da **sami nasumično generišete i proverite sigurnost vaše šifre bez korišćenja onlajn sajtova i programa.** Ukoliko vas mrzi da ručno računate entropiju vaše šifre, možete posetiti https://goo.gl/9OyNMY sajt koji vam neće tražiti da unesete vašu šifru, već podatke o njoj (da li koristite slova, brojeve specijalne karaktere i koje je dužine šifra).

Osim mrežnih merača sigurnosti i jačine šifara, na netu se mogu lako naći i gomile pravih korisničkih šifara koje su pribavljene u raznim neovlašćenim pristupima sajtovima i njihovim bazama podataka. Jedna takva baza podataka sa šiframa je javno dostupna na githabu https://goo.gl/VCbGj9. A za više o najkorišćenijim šifrma posetite http://wpengine.com/unmasked/.

Kada pravite šifre ili fraze, trudite se da imaju 80 ili više bitova entropije, da koristite i mala i velika slova, brojeve i specijalne karaktere nasumično odabrane. Fraze birajte isto nasumično iz nekog rečnika, odaberite da fraza ima najmanje četiri nasumične reči. Za svaki nalog pravite novu šifru/frazu, nikako nemojte upotrebljavati jednu istu šifru/frazu za više naloga, novi nalog totalno nova nezavisna šifra/fraza. Koristite neki menadžer šifara (eng. *password manager*) otvorenog koda. Nikako nemojte zapisivati šifre/fraze na papir, ili ih čuvati u ljudski čitljivoj tekstualnoj datoteci.

Kako sigurno čuvati šifre?

Menadžeri šifara

Prosečan internet korisnik ima više od 10 različitih naloga (zavisno od istraživanja prosečan broj se kreće od 17 do 27 https://goo.gl/oZ4B14, https://goo.gl/tzFzUQ). Taj broj tačnih šifara nije lako pamtiti, a pogotovo može biti teško zapamtiti koja šifra je za koji nalog. Da bi se običnom korisniku olakšao svakodnevni život, u sajber svetu postoje **menadžeri šifara** (eng. *password manager*). Ono što je još važnije, među njima postoje i oni koji su otvorenog koda. Menadžeri šifara će za vaš nalog generisati nasumičnu šifru/frazu željene dužine i sigurnosti, čuvati je u šifrovanoj bazi sa ostalim nalozima. Baza svih

vaših naloga se šifruje jednom šifrom koju morate zapamtiti. Prednost menadžera šifara je u tome što pamtite jednu šifru umesto za svaki nalog posebno. Preporučujemo Kipasiks (eng. *KeePassX*, https://www.keepassx.org/) ili Kipas (eng. *KeePass*, http://keepass.info/) koji postoji za Mek o.s. (eng. *Mac OS*), Vindouz (eng. *Windows*) i linuks, a postoji i Kipasdroid (eng. *KeePassDroid*, http://www.keepassdroid.com/) fork Kipas-a za android. Za ostale menadžere šifara možete posetiti stranice: https://goo.gl/XwKkJR ili našu skromnu listu manje poznati menadžera: https://goo.gl/pPUcjj). Postoje i grupni menadžeri šifara kao što su Timpas (eng. *TeamPass*, http://teampass.net/) i Pasbolt (eng. *Passbolt*, https://www.passbolt.com/) Kada koristite bilo koji menadžer šifara, napravite bekap šifrovane baze na nekom spoljnom sigurnom medijumu koji nećete davati svima.

Postoje i mrežni menadžeri šifara koji šifrovanu bazu šifara sinhronizuju sa nekim mrežnim serverom. Na taj način ukoliko izgubite svoj uređaj na kome ste držali šifre, i dalje možete pristupiti vašim šiframa skladištenim na serveru. Redundansa svih vaših šifara je zaista neophodna, pogotovo ako niste dobri u pamćenju šifara. Ovo ipak može predstavljati rizik po sigurnost vaših šifara jer pored sigurnosti vašeg uređaja, od velike važnosti je i način komunikacije sa serverom, sama bezbednost servera, kao i jačina šifre kojom ste šifrovali bazu šifara pre slanja na server. Takav je recimo Enkripter (eng. *Encryptr*, https://goo.gl/HdaeQR).

Mane menadžera šifara

Eventualne mane korišćenja menadžera šifara predstavlja centralizovano mesto koje sadrži sve vaše šifre, pa time predstavlja metu eventualnih napadača/hakera. Zatim pravljenje rezervne kopije i čuvanje iste na dovoljno bezbednom mestu, kao i eventualni propust u samom programu, može imati negativan efekat na sigurnost korisnikovih šifara. Napomenimo i to da je od

velikog značaja koji kriptografski algoritmi se koriste za šifrovanje baze šifara unutar menadžera, kao i koja se heš (eng. *hash*) funkcija koristi za čuvanje glavne šifre. Jer nisu svi kriptografski algoritmi sigurni (RC4 i DES, https://goo.gl/V8qD3h), kao što ni sve heš funkcije nisu sigurne (MD2 i MD4 i MD5, RIPEMD, https://goo.gl/LKzsDI.

Alternative menadžerima šifara

Da li morate da čuvate šifre uopšte? Da li postoji način da pamtite samo jednu sigurnu šifru i da na osnovu nje kreirate ostale, bez skladištenja bilo koje šifre na bilo kom računaru ili uređaju? Ovako nešto je zapravo moguće, štaviše veoma prosto. I ako ste pomislili da na jednu šifru samo nadovezujete po neki dodatni karakter (primer: *tajna_šifra123*, *tajna_šifra1234*), niste pogodili, ali bili ste blizu.

Koncept je sledeći:

1. Sastavite veoma dobru šifru ili frazu sa najmanje 80 bitova entropije (primer šifre: p:<(ZAS2O#PM ili fraze: dim livada mačka sir crveno prozor)
2. Odredite ime aplikacije ili sajta za koji sastavljate šifru (primer za sajt libre.lugons.org).
3. Odredite heš algoritme koje koristite za sastavljanje i eventualno dužinu šifre (primer koristićemo *base64*, *sha1*, i *sha256*)

Sada možete generisati šifru iz terminala po principu:
echo "šifra/fraza:ime_aplikacije/sajta" | base64 | sha1sum | sha256sum

```
echo  "ZAS2O#PM:libre.lugons.org"  | base64 | sha1sum | sha256sum
```

ili

```
echo  "dim livada mačka sir crveno prozor:libre.lugons.org"  |
base64 | sha1sum | sha256sum
```

Što će vam u prvom slučaju dati **29a6eac9c1a6800a886fdbdb7f8a2a36b4fc55994728ab9b37bdb01a7f1da107**, a u drugom **29a6eac9c1a6800a886fdbdb7f8a2a36b4fc55994728ab9b37bdb01a7f1da107**. Ovaj niz od 64 heksadekadna karaktera možete jednostavno smanjiti na željenu dužinu dodajući na kraj prethodnih komandi **tail -c 14** ili **head -c 10** (što će prikazati poslednjih 10 ili prvih 10 hedksadekadnih karaktera).

Kako da...?

```
echo "ZAS2O#PM:libre.lugons.org" | base64 | sha1sum | sha256sum |
head -c 10
```

Programi koji ovo rade postoje i to su Master pasvord (eng. *Master Password*, https://goo.gl/R6t2BI GPLv3), pvdheš (eng. *PwdHash*, https://goo.gl/jagYyt) i SuperGenPas (eng. *SuperGenPass*, https://goo.gl/4PtFO0 GPLv2). Svi su otvorenog koda, a Master pasvord i SuperGenPas su dostupni i kao android i Ajos (eng. *IOS*), veb-aplikacije, C program, i druge platforme (https://goo.gl/rQTCPX).

Ovaj sistem generisanja i čuvanja šifara ima prednosti kada je reč o skladištenju šifara, jer ono ne postoji. Ako vam neko ukrade računar, na njemu se ne nalaze vaše šifre uopšte. Ukoliko neko sazna šifru za jedan nalog, pomoću nje ne može saznati ostale šifre, ovako generisane, kao ni glavnu šifru od koje se sve ostale prave sve dok koristite sigurne heš algoritme. Napomena je da pogledate koji su heš algoritmi sigurni (https://goo.gl/LKzsDI), kao i da ne koristite samo base64 kodiranje, navedeno u prethodnom primeru, (ako ne znate šta radite) jer base64 nije heš funkcija i lako se može dekodirati . U navedenom primeru base64 se ipak koristi, ali posle njega se primenjuju dve dovoljno sigurne i ireverzibilne heš funkcije. Savet je da za heš funkcije koristite SHA256, SHA512, prihvatljive su i SHA1, RIPEMD160 i Virpul (eng. *Whirpool*) dostupni unutar OpenSSL-a, a ako ste pravi paranoik koristite BLAKE2 (https://blake2.net/), ali po cenu udobnosti i prenosivosti. Vrlo je važno odabrati dobru glavnu šifru, kao i sigurne heš algoritme, jer od njih zavisi sigurnost svih vaših šifara generisanih na ovaj način. Naravno, postoje određene mane uglavnom vezane za menjanje već postojećih šifara, jer zahteva pamćenje još jedanog podatka (da korisnik pamti i broj koliko puta je promenio šifru za određeni sajt) što može biti veoma nezgodno sa porastom broja naloga koji aktivno koristite. U tom slučaju bi algoritam izgledao

otprilike ovako:
šifra/fraza:redni_broj:ime_aplikacije/sajta" | base64 | sha1sum | sha256sum

Druga mana je što ćete morati brzo promeniti sve šifre ukoliko napadač sazna vašu glavnu šifru. Primetite da način na koji generišete šifre nije tajna, i napadaču neće značiti mnogo informacija koje heš algoritme koristite dok god su oni sigurni, i dok god je vaša glavna šifra dovoljno komplikovana.

Generatori šifara i fraza

Pomenućemo da za linuks postoje veoma korisni CLI programi poput pvgen-a (eng. *pwgen*) koji vam pomaže da generišete nasumične šifre (koga kada instalirate možete koristiti recimo ovako: **pwgen -sy 20 15** i koji će vam ponuditi 15 različitih, nezavisnih i nasumičnih šifara, gde je svaka šifra dužine 20 iz skupa od 95 karaktera). Tu je i pasvord gnerator (eng. *password-generator*, https://goo.gl/Suigwo) koji može generisati šifre koje se lako pamte **password-generator -l 20**Ili jednostavnije, bez instaliranja dodatnih programa

```
openssl rand -base64 20
```

ili

```
</dev/urandom tr -dc  ')(*&~^%$#@_:}[}],.?-|
~+=><\/`";!0123456789_A-Z-a-z'  | head -c20;
```

Za generisanje fraza možete koristiti Iks-kej-Si-di-pas (eng. *xkcdpass*, https://goo.gl/d8TJrB) i dobiti lako pamtljive fraze poput ove:

```
Yeti permutes kilobyte visa string
```

Zaključak

Kako ćete generisati i gde ćete čuvati šifre je svakako na vama. Upotreba sigurnih šifara nije teška, i programi poput Kipas-a i SuperGenPas-a to olakšavaju maksimalno. Svakako se isplati malo se potruditi oko svojih šifara, ne zato što nešto krijemo, već da nas ne bi bolela glava kada neki haker provali tajnu šifru „**password1234**".

Oslobađanje

Naredbe u GNU-Linuksu

(2. dio)

Autor: Adrijan Đurin

Nakon višegodišnjeg korištenja naredbi iz prvog dijela ovog serijala članaka, krajnje je vrijeme da se nauče nove naredbe. Kretanje kroz direktorije (**cd**) i izlistavanje njihovog sadržaja (**ls**) se jako često koriste, a ponavljanje je majka znanja - a i od glave višak ne boli. U nastavku članka pozabavit ćemo se stvaranjem. Jer, tko ne voli stvarati? Kreirati prazan fajl može se na više načina, a jedan od njih je naredbom **touch**.

Ako se nalazimo u direktoriju u kojem želimo kreirati prazan fajl, to radimo naredbom **touch <ime_fajla>**. Naprimjer, želimo kreirati popis stvari koje želimo kupiti u mjesnoj prodavaonici svega i svačega:

```
touch veoma_lijep_popis.txt
```

Naredbom za izlistavanje **ls** možemo provjeriti postojanje fajla. Fajl je prazan i spreman da u njega upišemo sve želje i zahtjeve - uz cijene, naravno. Kako bismo upisali bilo što u taj fajl, moramo se poslužiti novom naredbom. Nano predstavlja veoma jednostavan uređivač teksta unutar ljuske linuks sustava. Dostupan je na velikoj većini distribucija.

```
nano veoma_lijep_popis.txt
```

Izvršavanjem te naredbe otvara nam se jednostavno sučelje. Upisivanje se vrši tipkovnicom, i uz malo truda vaš popis može izgledati kao na slici.

[1] – ime fajla [2] – popis [3] – keyboard shortcuts, jer nema alatne trake

Kako biste brzo provjerili što se nalazi u vašem tekst-fajlu, a da pritom ne pokrećete Nano, upišite:

```
cat veoma_lijep_popis.txt
```

Rezultat je ispis vašeg tekst-fajla u terminalu. Naredba cat ima i neke druge posebnosti i razloge korištenja, ali o tome u kasnijim člancima.

Fajlovi i direktoriji čine okosnicu linuks sustava. Kreiranje direktorija također nije pretjerano teško. Postoji naredba za to. Pokušajte sljedeću:

```
mkdir igrice
```

Nakon toga izlistajte sve u trenutnom direktoriju. Pored svih standardnih direktorija, i prijašnjeg fajla, pojavio se i novi direktorij naziva „igrice”. Možete se prebaciti u njega pomoću naredbe cd da potvrdite da se radi o direktoriju - doduše, praznom direktoriju. Naredba

Oslobađanje

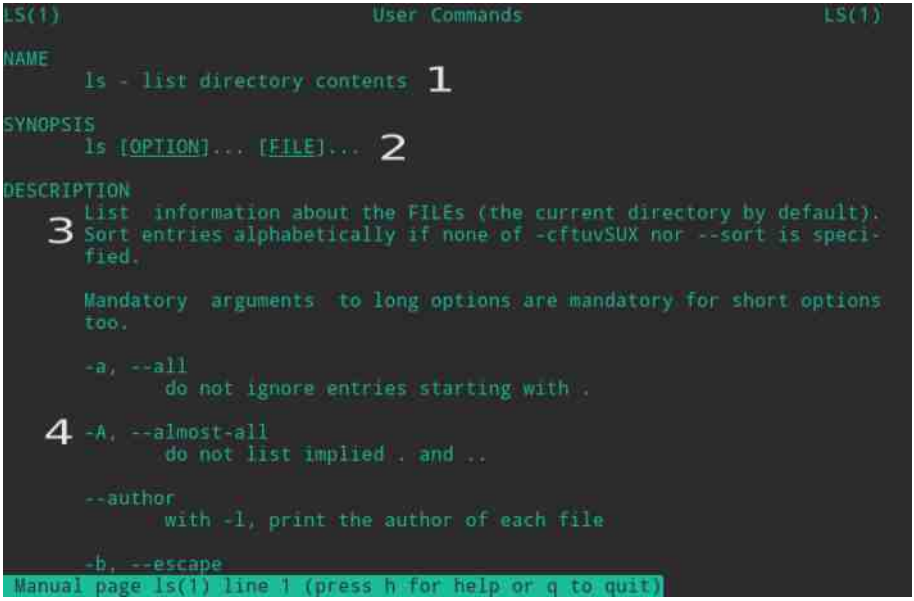
```
cd ..
```

vas vraća u prethodni direktorij.

Ukoliko niste sigurni što činiti, **man** naredba je zapravo *f1/help/malo_slabiji_google* za sve što trebate znati o pojedinim naredbama. Ona je priručnik u kojem se nalaze uputstva za upotrebu naredbi: što znači naredba, što radi i kako se koristi.

```
man ls
```

Ova naredba će nam otvoriti priručnik o **ls** naredbi, što možete vidjeti na slici.



[1] – ime naredbe [2] – kako se koristi [3] – opis naredbe [4] – dodatni argumetni (o tome u daljnjim člancima)

Kroz sučelje priručnika se krećete ili strelicama gore/dolje po jedan redak, ili tipkama f i b po cijelu karticu. Za izlazak iz priručnika koristi se tipka q. Isprobajte ovu naredbu i sa ostalim naredbama koje ste dosad koristili. Naravno, ako **man**

ne može pomoći onda vrlo vjerojatno može Gugl.

U ovom kratkom tekstu obrađene su naredbe koje su vezane za kreiranje fajlova (**touch**) i direktorija (**mkdir**), jednostavnu obradu teksta (**nano**) i naredbe koja nam služi kao priručnik ukoliko zaboravimo sintasku/svrhu određenih naredbi (**man**).

I, za kraj, evo nekoliko naredbi da se malo zabavite i razmislite. Što se događa kad unesete sljedeće naredbe:

```
nano neki_drugi_popis.txt

man man

mkdir Moje pjesme
```

Pregled popularnosti Gnu-Linuks i BSD distribucija u poslednjih šest meseci

Distrowatch

1	Mint	2769<
2	Debian	1795>
3	Ubuntu	1413>
4	openSUSE	1357=
5	Manjaro	1356>
6	Zorin	1043>
7	Elementary	1035>
8	Fedora	1029<
9	Deepin	825>
10	CentOS	791=
11	Antergos	785>
12	Arch	727=
13	Solus	687>
14	PCLinuxOS	621=
15	ReactOS	542>
16	Ubuntu MATE	531>
17	Mageia	518=
18	Lite	501>
19	KDE neon	480=
20	Lubuntu	476>
21	LXLE	470=
22	Puppy	438=
23	Kali	424>
24	antiX	415=
25	Tails	412=

Pad <
Porast >
Isti rejting =
(Korišćeni podaci sa Distrovoča)

Oslobađanje

Novi život starog računara

Autor: Igor Stoiljković

Jeste li ikada pomislili šta biste sve mogli uraditi sa starim kompjuterom čija je prva mladost davno prošla? Baciti ga? Da je tako ne bismo pisali ovaj tekst. Pokloniti ga starijim ili mlađim generacijama u vašoj porodici/familiji? E to je već nešto i ima neke veze sa ovim tekstom. Zašto se, uz malo uloženog truda, ne biste rešili vašeg starog računara (u neku ruku) i podarili vašem detetu ili već nekome drugome kome će prvi informatičarski koraci možda promeniti život?

Normalna je čovekova osobina da teži efikasnosti i upravo tom činjenicom možemo objasniti napredak čovečanstva; od prostih sekira i noževa od kamena do nuklearne fuzije, mobilnih telefona jačih od superkompjutera osamdesetih godina i Trikordera. Za autora ovog teksta, simbol efikasnosti je transformator jer je to najefikasnija mašina na planeti sa stepenom korisnog iskorišćenja do 98%.

Bacanje stvari koje još rade i koje mogu da se koriste u neku svrhu nije efikasano ponašanje i trebalo bi da se suzdržimo od takvog ponašanja. Ipak, živimo u Srbiji, zemlji čiji su građani preživeli razne pošasti tokom godina, od sankcija, ratova i inflacije do „skorašnje” tranzicije. Mogli bismo da se ugledamo na taj zapad i po tome što ćemo iskoristiti svaki dostupan resurs (efikasnost) a ne samo da postajemo konzumersko društvo poput njih jer ono su oni a mi smo mi, sa svime što to nosi.

No, vratimo se mi na iskorišćenje (starijeg) resursa. Ako posedujete računar koji ima bilo koji procesor sa dva jezgra, 1 GB RAM memorije, bilo koju grafičku kartu i 20 GB prostora na hard disku vi već imate solidno jak kompjuter i stoga prilično veliki izbor distribucija koje možete instalirati na svoj kućni računar. Praktično mogu sve ali neće sve biti sa zadovoljavajućom odzivnošću i brzinom. Neke distribucije mogu raditi već sa procesorom od 500 MHz i već sa manje od 128 MB

radne memorije, ali autor teksta vam ne preporučuje manje od 512 MV ako baš ne morate jer ipak ne pričamo o kompjuterima iz dosta starijeg perioda i zadovoljstvo korišćenja takvog sistema je diskutabilno (prim.aut.).

Za početak treba pogledati kakav hardver imamo na raspolaganju. Zatim se raspitati o distribucijama i odabrati jednu ili više koje vam deluju kao dobar izbor. Pametna je ideja probati u živoj varijanti sve distribucije koje to podržavaju, a to je danas skoro svaka. Treba voditi računa i o „ukusima", tj. o radnim okruženjima (eng. *desktop environment*) i upravljačima prozora (eng. *window manager*). Ne troše svi resurse na isti način, i dok su neki prelepi i krcati ukrasima, takvi su „teži" za sistem (eng. *eye candy*), neki drugi su rudimentalni ali veoma brzi i upotrebljivi.

Primer prvih, lepih i gladnijih za resursima, bili bi Ka-De-E (eng. *K Desktop Environment*) i Juniti (eng. *Unity* - Ubuntuovo okruženje), i donekle Sinamon (eng. *Cinnamon*) i Mate (eng. *MATE*), mada su oni puno lakši od prvopomenutog dvojca. Jednostavniji a brži su Iks-Ef-Ce-E (eng. *XFCE*), El-Iks-De-E (eng. *LXDE*), Enlajtenment (eng. *Enlightenment*), Oupen-boks (eng. *OpenBox*), Fluksboks (eng. *Fluxbox*) i *JWM* koji je verovatno najbrži predstavnik ove grupe.

Po autorovom mišljenju, nezahvalno je ubeđivati vas da uzmete ovu ili onu distribuciju jer je to stvar ličnih preferencija i afiniteta, i to što nekome odgovara neka distribucija ne znači da će se i vama svideti ili vam odgovarati. Ipak, autor lično koristi Manjaro linuks (eng. *Manjaro*) i prilično je zadovoljan njime. Za one sa jačim hardverom koji vole lepo okruženje je preporuka Ka-De-E sa Plazma (eng. *Plasma*) okruženjem verzije 5. Za one sa slabijim hardverom je preporuka

Oslobađanje

Iks-Ef-Ce-E (eng. *XFCE*), Oupenboks ili Fluksboks.

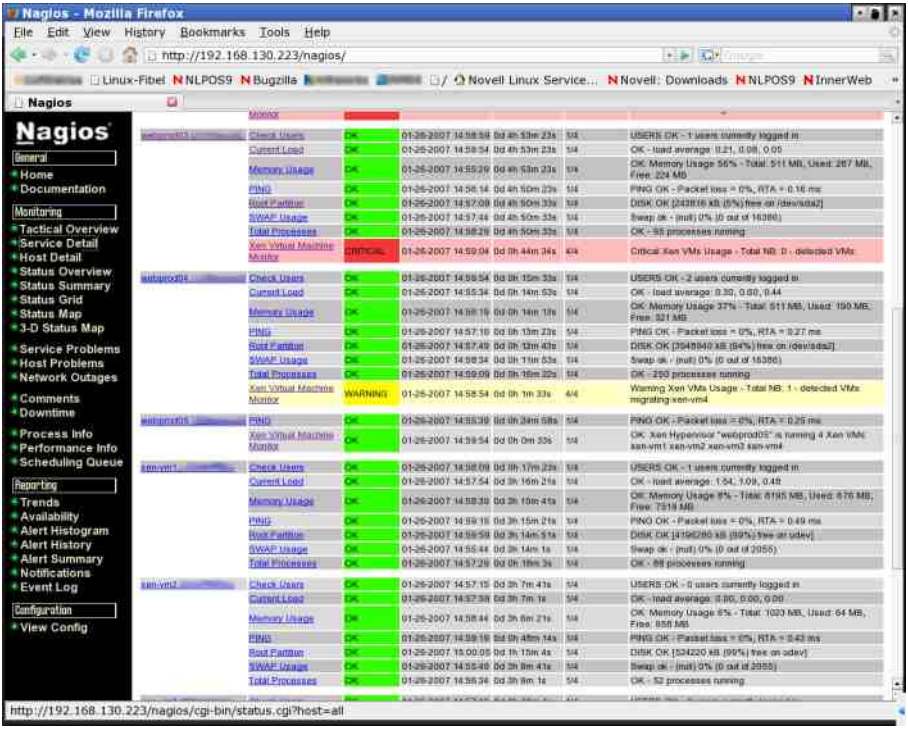
U suštini, ako vam se ne svidi Manjaro izaberite distribuciju koja vama odgovara ali se pridržavajte pravila o snazi hardvera navedenoj za Manjaro. Uživajte u svom novom starom računaru.

FAN

Sistem za nadzor servisa i uređaja

Autor: Stefan Biševac

Ako se bavite sistemskom ili mrežnom administracijom, a dugo tragate za nekomercijalnim rešenjem za nadzor i automatizovani oporavak vaše mrežne infrastrukture, onda će vam ovaj tekst definitivno olakšati u odluci za implementacijom jednog od najkorišćenijih rešenja otvorenog koda za monitoring računarske mreže – Nagios.



Slobodni profesionalac

Nagios je već dugo komercijalan proizvod koji nimalo nije jeftin za mala i srednja preduzeća, međutim, iz želje da ostane u kategoriji rešenja otvorenog koda, na zvaničnom sajtu Nagios projekta naći ćete takozvani Nagios Kor paket koji je potpuno besplatan. U ovom paketu sadržani su opšti fajlovi za konfiguraciju datoteka, skromna baza dodataka i veb stranica koja ilustruje status nadgledane infrastrukture. Ako ste početnik i ne poznajete sasvim dobro način funkcionisanja sistema za nadzor servisa, onda je najbolje da posetite ovaj sajt i tamo pronađete besplatne Nagios knjige koji detaljno opisuju Nagios Kor strukturu. Nagios je paket koji se instalira na jednoj od linuks distribucija (najčešće na onoj distribuciji kojom dobro vladate). CentOS je postao standard i omiljena distribucija mnogih sistemskih administratora pa je možda dobro rešenje da Nagios upravo podignete na CentOS-u zbog veoma bogate podrške za ovu distribuciju.

Ako ste do sada ipak imali prilike da radite sa Nagios Korom onda sigurno znate koliko je naporno definisanje novih računara, novih servisa i novih komandi jer se sve radi iz konzole, a Nagios fajlovi umeju da budu preobimni pa vam je za dobru konfiguraciju nekada potrebna izuzetna koncetracija. Nagios fajlovi su međusobno povezani pa je i za uočavanje najsitnijih grešaka nekada potrebno mnogo vremena. Najčešće greške javljaju se u nekoj standardnoj programerskoj formi, bilo da je to zatvorena vitičasta zagrada ili izostanak nekog slova u samoj skripti.

Nagios XI je komercijalno rešenje Nagios projekta koje sadrži u sebi veb stranicu za grafičko podešavanje sistema za nadzor. Statistika govori da je na ovaj način znatno olakšan posao administratorima u konfiguraciji i podešavanju svih mrežnih subjekata, čime se maksimalno izbegavaju greške u sintaksi pa se administrator mnogo više posvećuje suštinskoj konfiguraciji radi što boljeg podešavanja Nagiosa za nadzor svih delova mreže.

Prethodna distribucija Nagiosa je komercijalna i veoma skupa, međutim, grupa entuzijasta iz Francuske, a sada i iz celog sveta, radi na projektu FAN (eng. *Fully Automated Nagios*). FAN je zamena za Nagios XI, i prema iskustvu sistemskih inženjera, FAN nimalo ne zaostaje za Nagios XI distribucijom. FAN dolazi u obliku aplajensa i moguće ga je potpuno besplatno preuzeti sa ove stranice. On u sebi sadrži 3 nezavisna projekta: Nagios Kor, Centreon i NagVis.

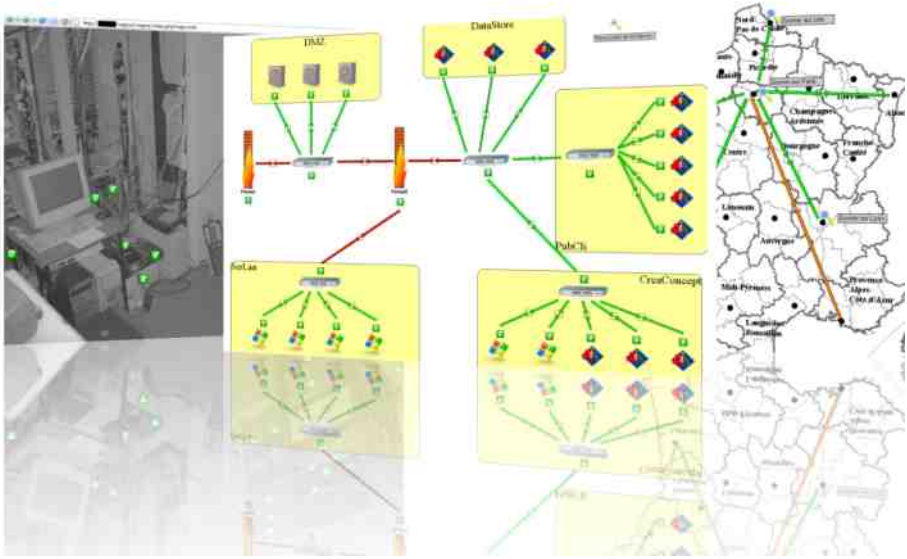
- Nagios Kor je srce ovog sistema. Zadužen je za obradu svih informacija i

obaveštavanje administratora o problemima u mreži. Ukoliko iskoristite i njegov ivent hendler onda dobijate potpuno moćan sistem nadzora koji može sam da odlučuje u određenim situacijama.

- Centreon, snažan sistem konfiguracije koji se javlja u vidu veb okruženja. Znatno olakšava posao unošenja novih subjekata u sistem za nadzor ili modifikaciju postojećih.

Slobodni profesionalac

- NagVis, predstavlja sistem za vizuelizaciju podataka. Ukoliko u vašoj organizaciji postoji veliki panel ili TV na kojem pratite stanje servisa, tada vam NagVis može mnogo jasnije pokazati šemu vaše infrastrukture na kojima se nalaze servisi koje sami definišete.



Ukoliko se još uvek razmišljate oko sistema za nadzor, tada je naša topla preporuka da što pre zaronite u svet linuksa i Nagiosa i za vašu organizaciju uspostavite snažan sistem nadzora i automatizovanog oporavka kritičnih servisa.

Ako nemate strpljenja da čitate obimne knjige na engleskom jeziku, onda pratite LiBRE! stranicu jer ćemo u narednim člancima objasniti detaljnije svaki od delova FAN projekta ponaosob, sa osvrtom na bitne činjenice koje bi trebalo znati kada je nadzor računarske infrastrukture u pitanju.

Kripto-ratovi (2. deo):
Nekada i sada

Autor: Petar Simović

Kliper čip

Američka nacionalna sigurnosna agencija (NSA) se nije zaustavila samo na slabljenju softvera, nego je prešla i na hardver, tačnije čipove i procesore. Ovo je i razumljivo jer su prvu bitku za softver i algoritme svakako dobili aktivisti i sajberpankeri, a proizvodnja hardverskih komponenti neophodnih za generisanje kriptografskih ključeva je bila u vlasništvu velikih kompanija podložnih uticaju države i tajnih službi. Kliper čip (eng. *Clipper Chip*) je bio projekat NSA agencije

devedesetih godina prošlog veka sa ciljem da se u mobilne telefone ugradi čip namenjen za šifrovanje zvučne komunikacije. Problem je u tome što bi tajni ključ određivao proizvođač čipa i tajno ga prosleđivao NSA agenciji koja je i dizajnirala algoritam po kome bi radio Kliper čip i koji je takođe bio tajna. Na ovaj način NSA bi bez ikakvog truda jednostavno dešifrovala svu telefonsku šifrovanu komunikaciju jer je znala tajne ključeve svakog uređaja. Vlada je u saradnji sa

NSA agencijom pokušala da primora sve telefonske kompanije da ugrade ovaj čip u svoje telefone, ali to nije uspelo. Takođe, Mat Blejz (eng. *Matt Blaze*) je uspeo da provali i zaobiđe ovaj sistem 1994. godine. Ako ovde zastanemo jer je već počeo dvadeset i prvi vek, možemo reći da su prve kripto-bitke dobijene, ali ratovi se nastavljaju i dalje, samo malo neprimetnije. NSA je nastavila da obogaljuje kriptografske protokole i ugrađuje specijalne čipove u hardver.

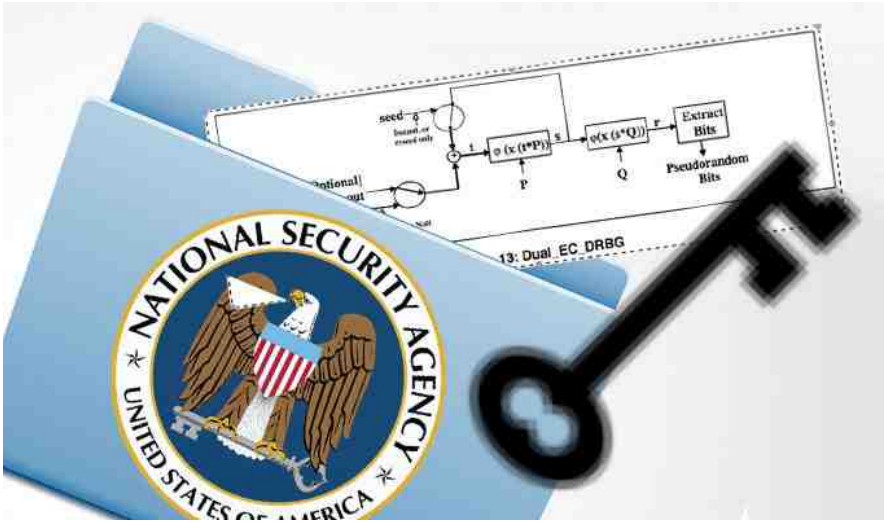
RdRand

NSA je kasnije podrivala sigurnost kriptografije na nižim nivoima. Većina softvera koja je implementirala neku kriptografiju je bila otvorenog koda i dostupna za proveru svakoga ko je to želeo da uradi. Takav primer je recimo *OpenSSL* koji implementira najjaču poznatu kriptografiju i masovno se koristi na serverima za sigurnu komunikaciju korišćenjem simetričnog, asimetričnog šifrovanja i kriptografskih heš (eng. *Hash*) algoritama za autentifikaciju. Oupn-Es-Es-El se oslanja na druge sistemske programe za generisanje „nasumičnih" brojeva koji su potrebni za pravljenje sigurnih tajnih ključeva, a baš to je i mesto koje je NSA napala kako bi ovaj protokol učinila manje sigurnim. Radi se o generatoru nasumičnosti (*Rd_Rand*, https://en.wikipedia.org/wiki/RdRand) unutar Intelovih procesora koji vraća pseudoslučajne brojeve, a za koga je počelo da se sumnja od 2013. godine da je modifikovan kako ne bi vraćao „nasumične" brojeve, već brojeve koji se mogu lakše predvideti. Ova tema stvorila je podelu i unutar Linuks zajednice jer je Linus Torvalds odbacio sumnje u narušavanje bezbednosti, dok je Fri-Bi-Es-Di prestao da koristi sumnjivi generator u jezgru svog operativnog sistema (izvori: https://goo.gl/LjHNYV, https://goo.gl/WsBHg3)

Dual_EC_DRBG

Kada smo već kod generatora „nasumičnih" brojeva, *Dual_EC_DRBG* je algoritam za kreiranje „nasumičnih" brojeva za eliptičke krive (eng. *Elliptic Curves*). Eliptičke krive se koriste za generisanje asimetričnih ključeva iste sigurnosti ali manje veličine nego *RSA*, i danas su najzastupljenije za uspostavljenje sigurne komunikacije na internetu, tj. unutar *HTTPS* protokola koji svakodnevno koristimo. Kao što možete pretpostaviti, ovaj algoritam (*Dual_EC_DRBG*) je konstruisala NSA i predložila ga Američkom Nacionalnom institutu za standarde i tehnologiju (eng. *National Institute of Standards and Technology*, *NIST*), koji biva usvojen i od ovog instituta i od drugih relevantnih sigurnosnih kompanija kao

siguran algoritam. Naravno, od samog pojavljivanja ovog sumnjivog algoritma, objavljivane su brojne publikacije koje su ukazivale da je algoritam nesiguran i to verovatno namerno bekdorovan (eng. *Backdoor*) (https://goo.gl/vQuHLL, http://goo.gl/8EJp12). Nesigurnost algoritma je potvrđena i dokumentima koje je Edvard Snouden (eng. *Edward Snowden*) izneo u javnost i koji su objavljeni 2013. godine kroz tajni program pod kodnim nazivom Bulran (eng. *Bullrun*) ozloglašene NSA. Bulran je samo jedan u nizu ovakvih tajnih programa koji sprovodi NSA kako bi na sve načine slabila i dešifrovala svu zaštićenu komunikaciju fajlovima (https://goo.gl/aauXwb). Prošle godine je objavljeno da je *Dual_EC_DRBG* bio takođe prisutan u SkrinOS (eng. *ScreenOS*) operativnom sistemu (eng. *firmware*) popularnog fajrvola (eng. *firewall*) sistema NetSkrin (eng. *NetScreen*) (https://en.wikipedia.org/wiki/Dual_EC_DRBG#cite_note-54)



U dokumentima koje je Snouden izneo u javnost, putem raznih medija i Vikiliksa, vidi se da je NSA nastavila da ugrađuje hardverske implante u matične ploče servera, u-es-be-ova i drugih kablova. Da stvar bude gora, ovo su radili presrećući pošiljke namenjene određenim osobama sa kupljenim ispravnim hardverom u koje su na tajnim lokacijama ugrađivali i podmetali svoje implante. Ovo je lepo dokumentovano sledećim video materijalima gospodina Apelbauma (eng. *Jacob Appelbaum*) sa jedne CCC konferencije: https://goo.gl/GwC8s9 i https://goo.gl/Ymv2Gb.

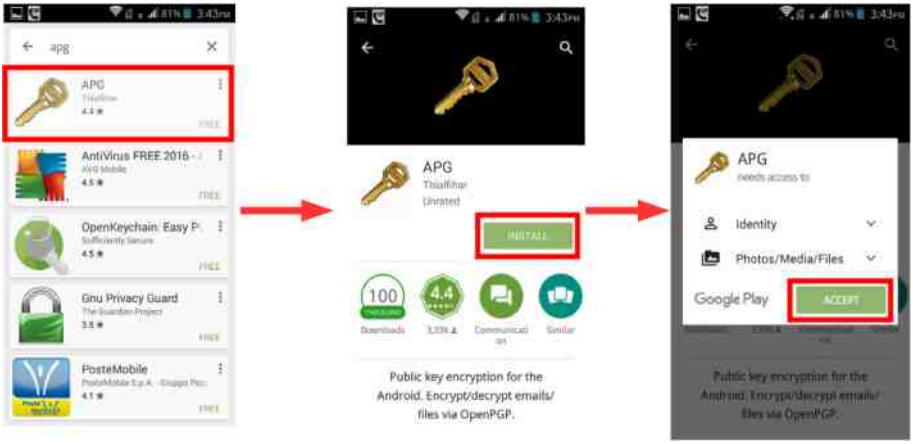
Šifrovanje elektronske pošte na Android-u: K-9 i APG

Autor: Petar Simović

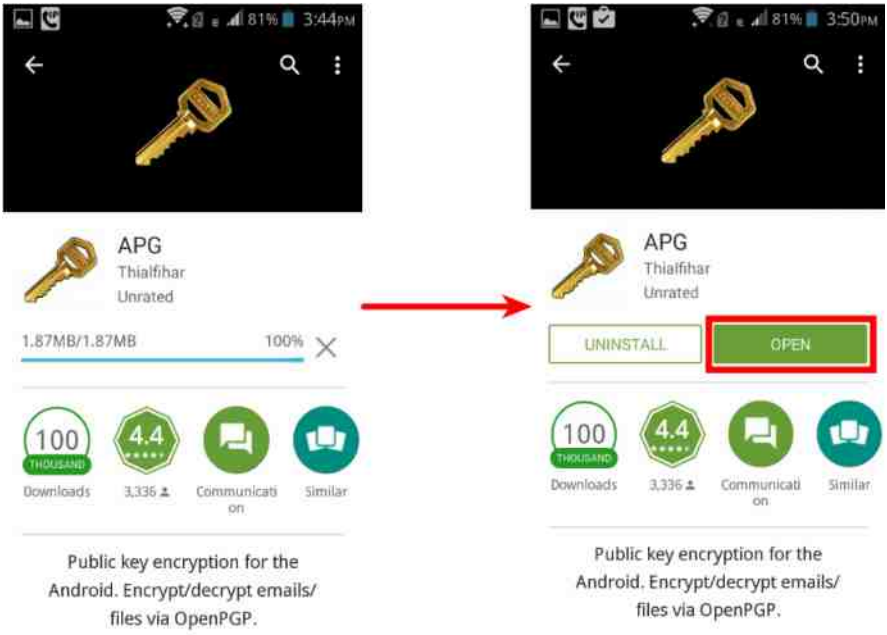
Svi koristimo imejl da komuniciramo, ali kako da sa lakoćom razmenjujete šifrovanu elektronsku poštu na vašem android telefonu koristeći vašu postojeću imejl adresu? Da biste mogli i na Androidu da primate i šaljete šifrovanu elektronsku poštu, potreban vam je program za manipulaciju GPG ili OpenPGP ključevima, kao i imejl klijent. Najbolje je da oba programa budu otvorenog koda (eng. *Open-Source*). Za imejl klijenta preporučujemo K-9Mail, a za GPG klijenta APG ili OpenKiČejn (eng. *OpenKeyChain*). K-9 mejl klijent će raditi sa oba ponuđena GPG klijenta, a možete ih preuzeti i sa Gugl Plej stora (eng. *Google Play Store*) i sa F-Droida (eng. *F-Droid*). Mi ćemo pokazati instalaciju, podešavanja i razmenu šifrovanih imejl poruka koristeći APG gpg klijenta i K-9 imejl klijenta.

Instaliranje APG-a

Ukoliko imate instaliran F-Droid, onda preporučujemo da APG preuzmete i instalirate sa F-Droida (https://goo.gl/IMzcOE), ili sa Gugl Plej stora (https://goo.gl/V38xkx).

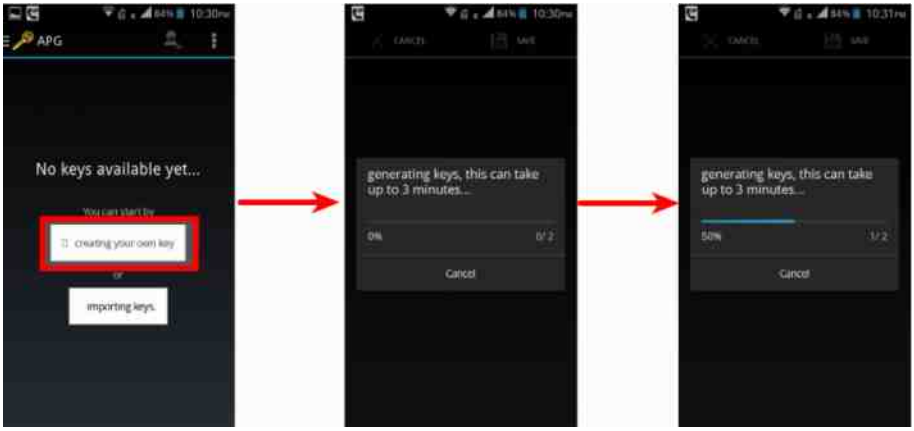


Kada se instalacija završi, pokrenite APG.

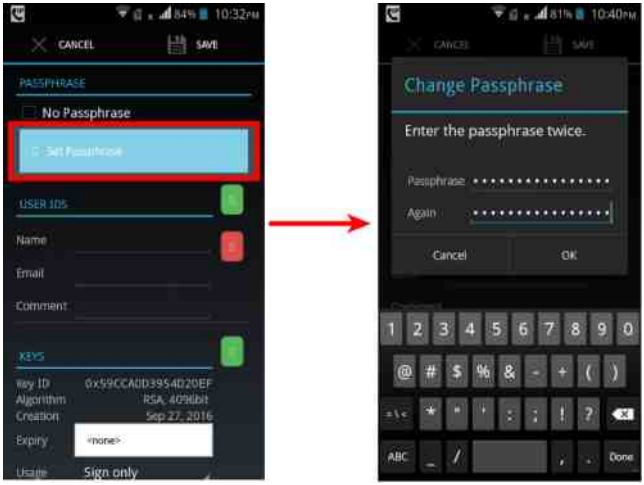


Podešavanje APG-a

Kada se instalacija završi, pokrenite APG kako biste generisali vaš novi GPG ključ za postojeći imejl.



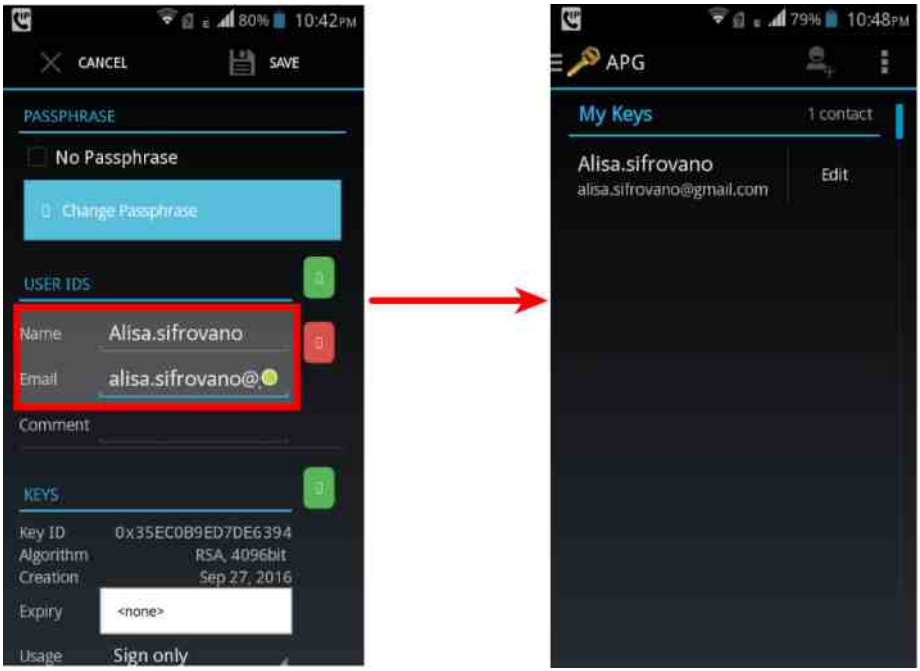
Odaberite opciju da kreirate vaš novi ključ (eng. *„Create your own key”*). Ukoliko već imate željeni GPG ključ za imejl adresu koju koristite i na Android telefonu, odaberite opciju za unos postojećeg ključa (eng. *„import keys”*) i unesite javni i tajni ključ sa drugog računara koristeći USB kabl.



Šifrovanje elektronske pošte na Androidu

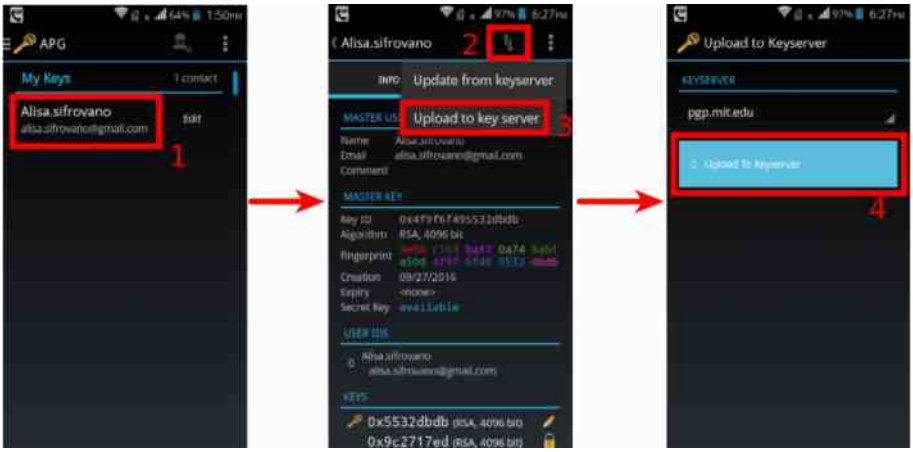
Kada se ključ generiše, pitaće vas da podesite GPG šifru za taj ključ. Ovde obratite pažnju jer šifra mora da bude jaka kako bi vas zaštitila i u slučaju gubitka ključeva. Šifra za pristup vašem imejlu ne bi trebalo da bude ista niti da liči na šifru koju ste podesili za vaš GPG ključ. Savetujemo upotrebu malih i velikih slova, brojeva kao i specijalnih kakraktera za šifru, kao i da dužina šifre bude preko 12 karaktera. Takođe je moguće umesto jedne duge šifre koristiti frazu od nekoliko nepovezanih slučajnih reči (kao na primer: *„Correct Horse Battery staple"*).

Nakon postavljanja šifre za novi GPG ključ, dodajte imejl adresu za koju ste generisali ključ, ime, kao i opcioni komentar ako želite. Posle ovog koraka smo završili sa podešavanjima za APG, i prelazimo na instaliranje i podešavanje imajl klijenta koji će se oslanjati na APG za operacije šifrovanja, dešifrovanja, digitalnog potpisivanja i provere digitalnih potpisa.



Objavljivanje vašeg javnog ključa

Kada kreirate GPG ključ, želite da objavite vaš javni ključ kako bi svako ko želi da vam pošalje šifrovanu poruku mogao lako da sazna i nabavi vaš javni ključ i njime vam šifruje poruku.

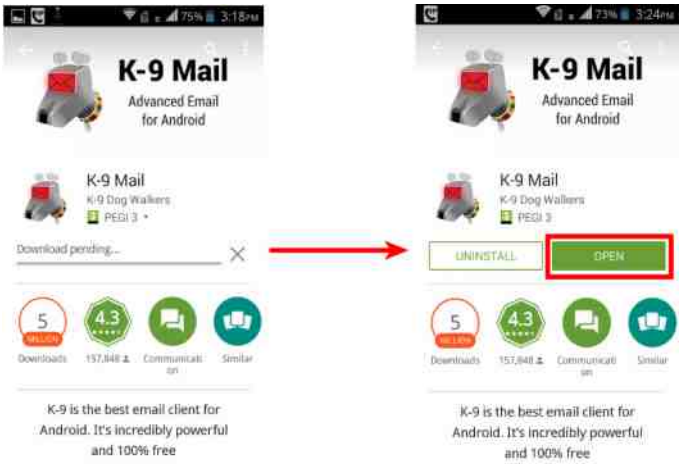


Pošaljite vaš javni ključ iz APG-a na server javnih ključeva (eng. *key server*), u našem slučaju server je (https://pgp.mit.edu/).

Instaliranje K-9 mejla

Kako biste lakše dešifrovali primljene šifrovane mejlove i slali šifrovane mejlove drugima, potreban vam je imejl klijent koji prepoznaje da se radi o šifrovanim porukama i u tom slučaju se obraća programu (APG-u) za podršku. Postoje i drugi klijenti pored K-9 mejla koji podržavaju šifrovanu elektronsku poštu oslanjajući se na APG ili Openkičejn (eng. *OpenKeyChain*), ali nisu otvorenog koda kao APG. Da biste instalirali K-9 mejl, idite na Gugle Plej stor (eng. *Google Play Store*, https://goo.gl/4tQTD), ili na F-Droid (https://goo.gl/yQejPh).

Kada se instalacija završi, pokrenite K-9 mejl.



Podešavanje K-9 mejla

Kada posle instalacije pokrenete K-9 mejl, potrebno je da podesite vaš imejl nalog unošenjem vaše imejl adrese (imejl adresa je ona ista za koju ste kreirali i GPG ključ, u našem slučaju alisa.sifrovano@gmail.com) i šifre za pristup toj mejl adresi. Važno je razumeti da postoje dve šifre: jedna za pristup vašem mejlu u

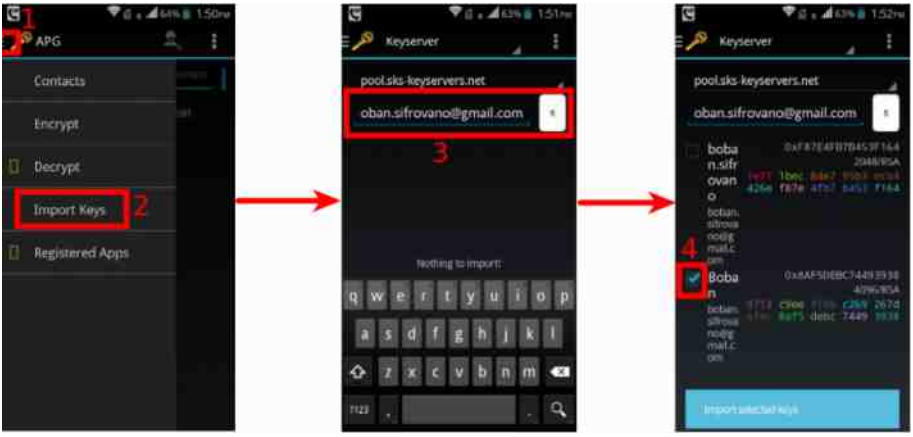
obliku korisničkog imena mejl adrese i šifre za to korisničko ime, a druga šifra je za pristup vašem tajnom GPG ključu koga ste malopre kreirali pomoću APG programa. Šifra za GPG nema nikakve veze sa šifrom za pristup vašem mejl nalogu, i ukoliko izgubite GPG šifru i dalje ćete moći pristupiti mejl nalogu i čitati/pisati nešifrovane mejlove.

U K-9 mejlu unesite imejl adresu za koju ste pravili GPG ključ i šifru za pristup tom imejlu.

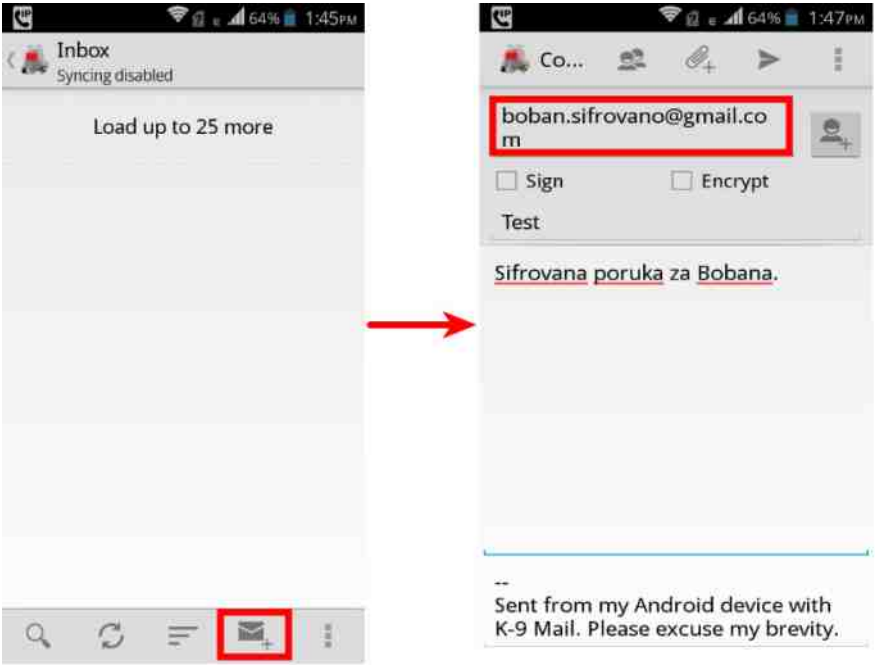
Razmena šifrovanih poruka

Nabavljanje javnog ključa kontakta

Da biste poslali šifrovanu poruku, potreban vam je javni ključ kontakta kome istu želite poslati, isti javni ključ vam je takođe potreban da biste proverili digitalni potpis primljene poruke istog kontakta. Pa hajde da preuzmemo javni ključ nekog našeg kontakta. Podrazumeva se da je i naš kontakt takođe kreirao svoj par GPG ključeva, kao i da je poslao javni ključ na neki server javnih ključeva. Napomenimo da nije bitno na koji server javnih ključeva ste vi poslali vaš javni ključ ili vaš kontakt jer se svi serveri javnih ključeva međusobno sinhronizuju. Pa tako, svaki ključ koji se pošalje na neki server javnih ključeva naći će se na svim ostalima posle otprilike desetak minuta.

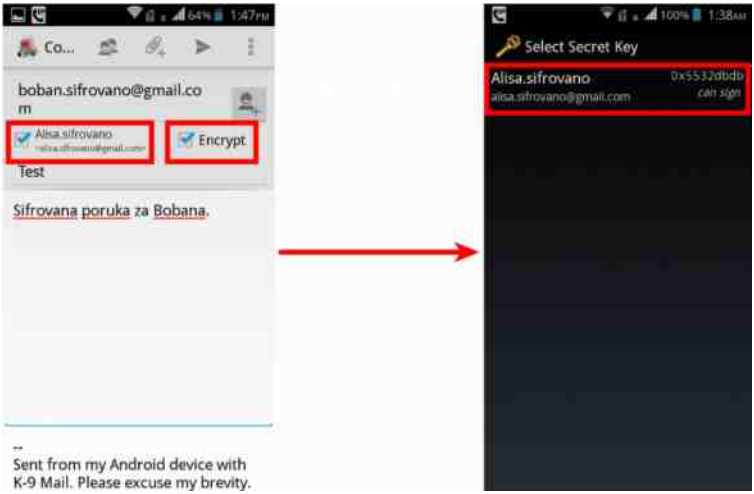


Slanje šifrovanih mejlova

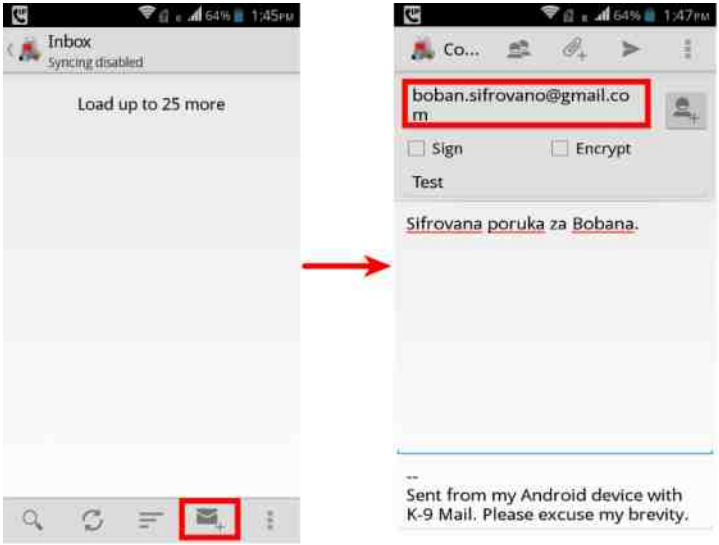


Mobilni kutak

Da biste poslali šifrovanu poruku, prvo sastavite istu i unesite imejl adresu primaoca čiji ste javni ključ prethodno preuzeli.



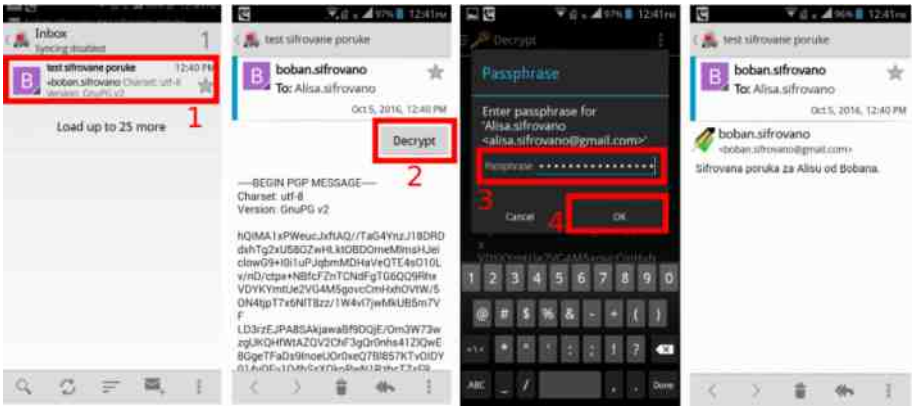
Kada sastavite poruku, odaberite opcije za digitalno potpisivanje (eng. *Sign*) i šifrovanje (eng. *Encrypt*), i selektujete za potpisivanje vaš ključ.



I najzad, kliknite na ikonicu za slanje poruke (papirni avioničić) i unesite vašu šifru za pristup vašem tajnom GPG ključu kako biste pristupili istom i digitalno potpisali poruku pored šifrovanja.

Dešifrovanje primljenih poruka

Kada vam neko pošalje šifrovanu poruku, potrebno je da otvorite K-9 mejl klijenta, otvorite primljenu poruku, kliknete na dugme za dešifrovanje (eng. *Decrypt*) i unesete vašu GPG šifru. APG prepoznaje šifrovane poruke unutar K-9 mejl klijenta i ponudiće da ih dešifruje.

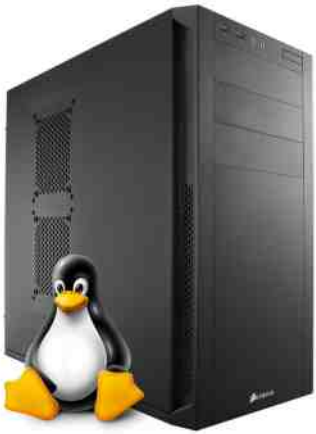


Kada primite šifrovanu poruku u K-9 mejl klijentu, kliknite na „Dešifruj” (eng. *Decrypt*) i unesite GPG šifru i to je to.

Hardver

Sastavi sam svoj Linuks kućni računar

Izbor najboljih komponenti za 2016-tu godinu



Autor: Nenad Marjanović

Sve je manje korisnika koji izdvoje svoje vreme da bi se posvetili odabiru komponenti za sklapanje kućnog računara. Sem ako, naravno, izuzmemo zaljubljenike u video igre. Prvi faktor je svakako nedovoljno poznavanje hardvera i tehničkih veštine koje su ipak neophodne da se sve sastavi, instalira i izvrši podešavanje operativnog sistema. Takođe, tu se ponekad može isprečiti cena i faktor odlučnosti oko izabira komponenti. Korisnici se uglavnom odlučuju za kupovinu prenosnih računara zbog njihove praktičnosti i zahteva koju donose današnja komunikacija i poslovne obaveze.

Za one koji ipak znaju da kvalitet dolazi sa znanjem, na osnovu iskustva linuks korisnika širom sveta naša redakcija je napravila selekciju komponenti koje ćemo predstaviti u ovom članku. Za istraživnje linuksa dovoljno je kupiti i Rasberi Paj (eng. *Raspberry Pi*), a za malo naprednije korisnike konfiguracije mogu dostići i cenu od par hiljada evra.

Matična ploča

Pri izboru matične ploče treba razmišljati o nekoliko važnih detalja. Da podržava poslednju generaciju procesora (*LGA1151*), da je modularna (ovo označava da vremenom možemo dodati komponente koje nismo mogli uključiti u konfiguraciju na samom početku) i, na kraju, broj konektora za spoljašnji hardver kao što su HDMI/VGA i USB poslednje generacije, 3.0. Što se tiče formata, danas se većina korisnika odlučuju za mikro a-te-iks (eng. *micro ATX*). Razlog ovome je što u kombinaciji sa manjim kućištima ovako montirani računari zauzimaju malo prostora i mogu stati na bilo koji radni sto i ujedno nivo buke je minimalan. Gigabajt *GA-Z170M-D3H* poseduje sve ove predispozicije i podržaće sve moderne linuks sisteme. Kada govorimo o podršci, u to spadaju čipsetovi (eng. *chipset*) koji imaju odličnu podršku za bežični internet i zvuk. Cena ove matične ploče se kreće oko 120 evra.

Hardver

CPU (procesor)

Vreme je da se posvetimo izboru srca našeg budućeg računara. Opredelili smo se da zadovoljimo svačije ukuse, od korisnika koji isključivo koriste računar za posetu internet portala, do onih koji bi želeli da imaju mogućnost za pokretanje virtualnih mašina u cilju učenja administracije sistema do osoba zainteresovanih za pentesting i istraživanje sigurnosti sistema i aplikacija. Naša odluka je Intel šeste generacija *i5* sa četiri jezgra na radnoj frekvenciji od 3.4 gigaherca (turbo mod omogućava modifikaciju frekvencije do 3.9 gigaherca). Model koji smo testirali je *i5-6600K*, čija je cena i dalje visoka (oko 220 evra) ali nosi sa sobom sve potrebne osobine procesora poslednje generacije. Ovaj procesor može služiti i ponosnim gejmerima.

RAM (memorija)

Do skoro smo svi pričali o DDR3 memoriji, ali kao što to biva u informatici vođeno Marfijevim zakonom, danas već imamo DDR4 memoriju. Za moćni procesor koji smo izabrali i da bismo iskoristili maksimalno njegove mogućnosti, izabrali smo dva puta 8 gigabajta Korsar (eng. *Corsair*) LPX DDR4. Cena ove memorije je oko 80 evra. Treba napomenuti da gorenavedena matična ploča može podržati do 32 gigabajta memorije.

HDD, SSD ili m.2

HDD i SSD su i dalje dobra kombinacija ako se odlučujemo oko kapaciteta i brzine. Većina korisnika danas koristi SSD za instalaciju sistema, a HDD za čuvanje podataka, međutim ovde govorimo o budućnosti i dugoročnom rešenju za naše potrebe, tako da se treba odluciti za SSD. Trenutno model koji nudi najbolje rešenje po pitanju cene i performansi je *Crucial MX* 250GB. Cena je oko 100 evra.

Kućište

Da bismo negde udomili sav ovaj lepi materijal potrebno nam je i kućište. Izbor je ogroman, ali na osnovu hardvera koji smo već predložili uzećemo kućište koje podržava format matične ploče, kao i alimentacije. Pri izboru kućišta bi trebalo, pored gorenavedenih faktora, proveriti mišljenja drugih korisnika da bismo bili sigurni da je nivo zvučne izolacije dovoljan da sa našim računarom možemo spavati u istoj prostoriji. Naravno, nivo buke ne zavisi samo od kućišta, ali dobro napravljeno kućište može ukloniti neminovan zvuk ventilatora koji su pomalo umorni od prevelike upotrebe. Na našim prostorima možemo pronaći Kuler Master proizvode, ali tu su i druge opcije. Svako kućište ispod 40 evra je u većini slučajeva lošijeg kvaliteta, tako da se treba dobro raspitati pre konačne odluke.

Napajanje

Uvek na napajanje treba gledati kao na motor koji će raditi ponekad i po nekoliko dana bez prestanka, a ako smo takvi korisici, onda invensticija od 65 evra ne bi trebalo da nas blokira pri izboru, već naprotiv, da nam obezbedi dugovečnost ostalih komponenti, svojim stabilnim radom. *Be Quiet! Pure Power L8 CF* je model od 500W. Ako imate novca za modularni model, nemojte se dvoumiti, zato što sa tim tipom napajanja u kućištu možemo ostaviti samo kablove koji su nam potrebni u datom trenutku, a ostale možemo ukloniti. Ovo ipak ostavljamo u domen estetike koja većini korisnika nije presudna pri odabiru.

Ventilator procesora

Ovo je deo, pored matične ploče, koji će pojedincima oduzeti dane u potrazi za najboljim rešenjem. Iako je sve više računara sa tečnim hlađenjem, što pre samo par godina nije bio slučaj zbog cene i tehničke izvodljivosti, danas se modeli vredni spomena kreću od 70 evra, ali to ćemo ostaviti na izbor iskusnijim građevinarima PC nebodera. Na testu smo skoro imali „manje" poznatu marku, koja odlično radi svoj posao, pogotovo ako ne volite da čujete dosadni šum koji dolazi iz kućišta.

Pri odabiru ventilatora treba voditi računa da podržava tip procesora koji koristimo i naravno broj decibela koji smo spremni da podnesemo, ili ne. *Be Quiet! Pure Rock*, i ako ste u mogućnosti da nađete verziju Blek, biće sasvim dobro rešenje.

Na kraju ostaje da zavrnemo rukave, dotaknemo neku metalnu površinu i sklopimo uređaj koji će vredno raditi u našim domovima.

http://cryptoparty.rs