Фебруар 2017. **Број 46**

ЛиБРЕ!

Часопис о слободном софтверу

Слободни софтвер у Босни и Херцеговини

ЈОШ ИЗДВАЈАМО

ФАН Систем за надзор сервиса и уређаја

Шифровање електронске поште на Андроиду: K-9 и АГП

Реч уредника

Промене

Велика пауза доноси велике промене. Данас када се навршава тачно пет година од идеје за покретање часописа, са поносом можемо да вам представимо 46. број часописа, уз који долазе радикалне промене.

Са погледом на прошлост, морамо признати да је статистика која се крије иза ових пет година заиста задивљујућа. Преко шездесет аутора је учествовало у реализацији 46 бројева као стални или повремени сарадници, а у тим бројевима је обрађено преко триста различитих тема о слободном софтверу. Ове чињенице нам нису дозволиле да одустанемо у моментима када је даљи наставак рада Часописа доведен у питање. Проблеме кроз које смо прошли у претходној години остављамо иза себе, и оптимистичним кораком настављамо даље. Поносни свим досадашњим успесима часописа и охрабрени подршком наших читалаца, увели смо одређене промене које ће одржати часопис активним сигурно још пет година, а надамо се и више.

Најзначајнија новина је дефинитивно још један облик ЛиБРЕ! часописа - на добро познатој адреси libre.lugons.org се налази ЛиБРЕ! блог. „Да ли ЛиБРЕ! треба да постане блог?" - питање је које се од самог почетка Часописа провлачило кроз редакцију. Након пет година то се десило; редакција је дошла до закључка да је то најефикаснији начин да се читаоцима омогући приступ ризници знања сачуваној у претходним бројевима. Овај потез је повукао са собом остале промене. Ако сте приметили да су вам чланци познати, разлог томе је нови начин објављивања. Сваки чланак пре него што се појави у пдф издању часописа премијерно ће бити објављен на његовом сајту. Поставља се питање чему онда даље објављивање нових бројева часописа. Нисмо желели да се одрекнемо предности које нам такво издање пружа, али пре свега смо решили да останемо доследни форми која нас прати од

самог почетка и чини јединственим.

Наредни број ће бити објављен тек кад се прикупи довољан број текстова, што ће изазвати одређене варијације у периодици излажења. Периодика објављивања часописа зато постаје неодређена, а нови број ће излазити као пресек текстова већ објављених на сајту. Посреднички формат за мобилне уређаје какав је еПУБ је изгубио свој смисао, тако да од овог броја, еПУБ издање часописа више неће постојати.

Такође, радикалне промене се могу приметити у функционисању ЛиБРЕ! тима. Ослобађањем притиска које је са собом носила обавеза објављивања новог броја једном месечно, надамо се да ћемо привући нове чланове у наш тим. Пројекат постаје мање захтеван за све његове чланове, што пружа могућност дужег рада на чланцима, а самим тим и повећање њиховог квалитета.

ЛиБРЕ! пројекат ће овиме доста успорити, али то ће му пружити могућност да се посвети осталим битним сегментима. Поред повећања квалитета текстова објављених у часопису, једна од главних тежњи биће повећање утицаја у региону. ЛиБРЕ! као регионални пројекат ће покушати убудуће да што више прикаже стање слободног софтвера и дешавања у региону, што се може већ видети у овом броју чланком који анализира стање слободног софтвера у Босни и Херцеговини. Наставиће се са објављивањем старих текстова; одређен део библиотеке знања је већ доступан на сајту, а у наредном периоду можете очекивати постепено објављивање и остатка текстова.

До следећег броја,

ЛиБРЕ! тим

Садржај

Моћ слободног софтвера

Број: 46

Извршни уредник: Никола Тодоровић

Главни лектор:
Адмир Халилкановић

Лектура:
Јелена Мунћан, Сашка Спишјак

Графичка обрада:
Дејан Маглов, Зоран Лазаревић

Дизајн: White Circle Creative Team

Аутори у овом броју:
Никола Тодоровић, Стефан Ножинић, Ненад Марјановић, Игор Стоиљковић, Марјан Ђуран, Амар Туфо, Адријан Ђурин, Стефан Бишевац, Момчило Медић, Петар Симовић

Почасни чланови редакције:
Жељко Попивода, Михајло Богдановић, Владимир Попадић, Жељко Шарић, Александар Станисављевић

Контакт:
IRC: #floss-magazin на irc.freenode.net

Е-пошта: libre@lugons.org
Веб: http:/libre.lugons.org

Вести

9.септембар 2016.

Балкон 2к16

Од 9. до 11. септембра, у Новом Саду, у конгресном центру, одржао се највећи хакерски конгрес на територији Балкана, Балкон 2к16. Четврти пут заредом, организатори су успели да превазиђу сами себе. За све који су пропустили овај догађај доступни су снимци са предавања.

Корисни линк: http://bit.ly/2m0HgAI

13.октобар 2016.

Убунту 16.10

Објављена је нова верзија популарне Линукс дистрибуције, Убунту 16.10. Најважнија промена је свакако нови Кернел верзије 4.8, који доноси велики број промена везаних за стабилност, брзину и енергетску ефикасност.

Корисни линк: http://bit.ly/2kWcJ5W

---

14. октобар 2016.

20. рођендан КДЕ

Заједница окупљена око КДЕ пројекта прославила је свој двадесети рођендан. Заједница, која је започета са намером да развија графичко окружење за линукс оперативне системе, данас развија велики број корисних алата, као и оперативни систем за мобилне телефоне.

Корисни линк: http://bit.ly/2kMMkXF

---

22. новембар 2016.

Федора 25

Федора оперативни систем је добила своје 25. издање, које садржи велики број исправки.

Корисни линк: http://bit.ly/2m0I1tx

24.јул 2016.

Кернел 4.9

Линус Торвалдс је објавио кернел 4.9, ово издање има највише промена до сада у односу на претходну верзију; извршено је чак 16 хиљада значајних промена у коду.

Корисни линк: http://bit.ly/2IjKG1H

16. децембар 2016.

Линукс Минт 18.1

Представљена је прва исправка 18. издања Линукс Минт оперативног система.

Корисни линк: http://bit.ly/2kMoLhE

17. децембар 2016.

Лугонс БарКамп 5

На Факултету техничких наука у Новом Саду одржан је пети по реду Лугоносов БарКамп, који се организовао у сарадњи са Катедром за Примењене рачунарске науке.

Корисни линк: http://bit.ly/2IXF1RL

Вести

24. децембар 2016.

Линеџ ОС

Након објављивања вести да се пројекат Сајногенмод (енг. *CyanogenMod*) гаси, група програмера решила је да настави пројекат, одвојено од компаније Сајноген И-ен-си (енг. *Cyanogen INC*), под називом Линеџ ОС (енг. *Lineage OS*).

Корисни линк: http://bit.ly/2m0D587

23.јануар 2017.

Сербиан Гну-Линукс 2017

Доступна је за преузимање четврто издање домаћег оперативног система Сербиан Гну-Линукс 2017, са КДЕ и Опенбокс графичким окружењем.

Корисни линкови: http://bit.ly/2kBGMUv
http://bit.ly/2m0BgI7

24.јануар 2017.

Вајн 2.0

Популарни програм за извршавање програма за Виндоуз - Вајн (енг. *Wine*) - објавио је нову верзију 2.0, са подршком за велики број нових апликација и игрица.

Корисни линк: http://bit.ly/2lwqJ9F

---

1. фебруар 2017.

Либреофис 5.3

Недавно је објављен Либреофис 5.3. Долази са уједначеном подршком за приказ текста на свим оперативним системима, и уз ког је објављено и прво издање Либреофис Онлајн (Лоол), веб верзије пакета која се може користити у оквиру локалне инфраструктуре.

Корисни линк: http://bit.ly/2IyTZx6

---

5. фебруар 2017.

Олимекс Терес I

Из Бугарске нам стиже потпуно расклопиви лаптоп отвореног хардвера, Олимекс Терес И. Лаптоп је предстсављен на Фосдему у Бриселу и може се поручити.

Корисни линкови: http://bit.ly/2IjCSwA
http://bit.ly/2Iza4Ty

Пулс слободе

Дескон 2016

Аутор: Никола Тодоровић
Фотограф: Владимир Опсеница

Након изузетно успешне прве пилот конференције Дескон 2015, ове године смо имали прилику да присуствујемо тродневној хакатон конференцији Дескон 2016 (http://descon.me/2016/). Као и прошле године, Дескон је организован у експерименталном уметничком простору ИТС-з1 (http://its-z1.org/) уметника Драгана Илића, у приградском насељу Ритопек, недалеко од Београда, а учесницима конференције је организован посебан превоз из београдског Хаклаба.

По узору на све веће хакерске конференције, Дескон је ове године имао свој бец. Међутим, оно што ју је издвајало од осталих јесте прилика да учесници конференције свој бец направе сами. Да не би дошло до забуне, важно је знати да се под

бецом сматра мало парче електронике. Уз помоћ екипе из хаклаба која је осмислила бец сваки учесник је уведен у свет електронике и упознат са основним вештинама лемљења и повезивање електронксих компоненти. Након добро обављеног хардверског дела, свако је требао испрограмирати свој бец притом искористивши бројне могућности које нуде Ардуино модули, а атеље у ком се дешавао већи део конференције додатно је поспешио креативност код учесника конференције.

Конференција је отворена уводном речју саме организаторке Жељке Десире (Дес) Милошевић, а остатак првог дана је прошао уз међусобно упознавање, припрему за прављење бецева и једно предавање. Предавање је одржао Душан Михајловић, слушаоцима рок музике осамдесетих познатији као „Др. Спира", и он је говорио о томе како усред потребе да се све дигитализује, због лоше компресије се губе битне информације које су подаци пре тога садржавали. Указао је на чињеницу да дигитална технологија не може све да квантификује и прикаже у облику нула и јединица.

Други дан смо имали прилику да чујемо предавање Метјуа Џексона, који је посебно за Дескон допутовао са Новог Зеланда у Београд. Метју нам је говорио о својим пројектима као и о старт-апу *Doctor2Go*, чији је он суоснивач. Након Метјуа, имали смо прилику да чујемо нешто о домаћем старт-апу Стробери енерџи од стране Кристине Николић. Кристина је представила њихове производе за паркове, који су познати као Стробери дрво и Стробери паметна клупа, а остатак предавања је протекао у коментарисању будућих пројеката старт-апа. Филип Дулић, креатор Дескон беца, је одржао кратко предавање као упутство за програмирање беца, након чега је софтверски изазов могао да почне.

Пулс слободе

Једна од главних атракција на имању уметника је дефинитивно била велика роботска рука која је служила уметнику Драгану Илићу као помоћ и замена у сликању. Током трајања конференције одржан је перформанс који уметник планира у наредној години да прикаже у музејима. Перформанс је настојао да представи и другу могућност роботске руке, облика музичког инструмента. Роботска рука је попут удараљке покушала да направи галаму лупајући по цевима и гвожђу окаченом о зид.

За време целе конференције била је активна криптографска загонетка, коју је саставио Петар Симовић, аутор текстова о криптографији и безбедности за ЛиБРЕ! часопис. Петар је уз помоћ осталих чланова Хаклаба одржао крипто-парти на ком су сви били упознати са начином како да се заштите од шпијунирања и како да шифрују своју комуникацију путем мејла. Да ни у једном тренутку не пропадне добра атмосфера побринула су се три ди-џеја, која су се смењивала сва три дана.

Предраг Радовић је започео трећи дан са предавањем о Етереуму, након чега је уследило предавање Петра Симовића о блокчеину (енг. *Blockchain*). Последњи дан је послужио за финализовање пројеката за бец и њихово презентовање, а жири је донео нимало лаку одлуку и доделио награду Метју Џексону за најбољу употребу беџа. Присуствовали смо јако лепом гесту, јер новчану награду за победника хакатона, коју је Метју обезбедио и освојио, на крају конференције је донирао Хаклабу. Конференција је завршена опуштеном атмосфером уз разговоре и обећања да ће и следеће године сви обавезно доћи.

Пулс слободе

Слободан софтвер у Босни и Херцеговини

Аутор: Амар Туфо

Данас, када слободан софтвер није више што је био прије двадесетак година када га је било јако тешко инсталирати и савладати његове основне кораке, јер га је користила углавном одређена скупина компјутерских ентузијаста - прича је потпуно другачија и слободан софтвер је постао доступан свима понудивши нам велики извор оперативних система који су намијењени како почетницима, тако и професионалцима. И, док у региону постоје активна линукс удружења која преносе своја знања и искуства међу корисницима, у овом чланку ћемо погледати стање заступљености слободног софтвера у Босни и Херцеговини.

Знају ли људи уопће шта је линукс?

Земље региона попут Србије и Хрватске веома успјешно прате трендове у свијету слободног софтвера. Управо успјешни портал Линукс За Све долази из Хрватске, а ЛиБРЕ! часопис, засигурно један од најбољих часописа о слободном софтверу, настао је у Србији. Они, поред промоције слободног софтвера, подстичу кориснике да сами заплове његовим водама, јер се веома често за линукс кориснике каже да су сами своји мајстори. Босна и Херцеговина тренутно је земља са највећим бројем информатички неписмених људи - како младих, тако и одраслих. Чињеница је да је информатика данас постала незаобилазан сегмент људског живота. Свјетска економија почива на интернету и сличним технолошким новитетима, који ничу сваки дан. Стога, када је ријеч о нашој земљи, скоро осамдесет процената људи веома слабо користи или познаје рачунаре и њихову терминологију. Тако је слободан софтвер само једно од „шпанских села". Сматрамо да таквом стању нашег друштва углавном доприноси школски образовни систем, али и веома лоше гласине о линукс оперативним системима: например, да су компликовани; да су намијењени само хакерима, програмерима; да нема подршке драјвера, и слично. С друге стране, кључну улогу „удаљавања" од истих поспјешују технички факултети те продавнице

компјутерске технике. Није све ни тако црно, па у овој нашој земљи можете пронаћи и велик број информатичких ентузијаста који спадају међу напредне кориснике рачунала, који програмирају, и који не користе рачунала само за разоноду. Тако се и сами изненадимо када сусретнемо људе који познају линукс, који га дуго користе и који знају његове предности у односу на конкуренцију. Морали бисмо овдје бити искрени и рећи да број тих људи није тако велики, али је похвалан. О томе колико је популација у Босни и Херцеговини информатички (не)писмена прочитајте на линку (http://ceppei.ba/bos/index.php?option=com_content&view=article&id=4874&Itemid=72)

Удружења Линукс корисника

У региону дјелују активно линукс удружења која несебично шире и преносе знање на друге; одржавају разне едукације, семинаре, дружења и то све у циљу побољшања информатичког образовања. Међу њима можемо поменути ЛУГоНС (Србија), ХУЛК (Хрватска), Убунту Србија, Убунту Хрватска, већ поменути портал Линукс За Све, као и ЛиБРЕ! часопис. Каква је ситуација у Босни и Херцеговини? Линукс удружења у БиХ нема много, барем не оних који су тако активна. Међутим, мало бољим претраживањем пронаћи ћете „Удружење Линух корисника БиХ" (http://www.linux.org.ba/), које је основано 1998. године. Удружење је активно промовисало употребу линукса, те одржавало и едукације у области линукса на Електротехничком факултету у Сарајеву. Удружење није активно посљедње

четири године због непознатих разлога. Такође, треба поменути УЛКРС (http://ulk.rs.ba/). За оне који не знају, ријеч је о Удружењу Гну-Линукс корисника Републике Српске, које је основано 27. јануара 2010. године, а које, нажалост, такође није више активно. Када је ријеч о другим удружењима, овдје можемо поменути она која дјелују и постоје искључиво на друштвеним мрежама, а која окупљају велики број линукс корисника и далеко су активнији. То су: Убунту Удруга БиХ, Имплементација Линукс ОС у Босни и Херцеговини те Убунту линукс група Босне и Херцеговине (енг. *The Linux OS Ubuntu group Bosnia and Herzegovina*). Ова три удружења, која углавном дјелују на Фејсбуку, вриједно промовишу употребу линукса и слободног софтвера у свакодневном животу, а окупљају близу пет стотина активних чланова, што је јако похвално.

Публикације и пројекти о линуксу

Код нас тренутно не постоји ниједан нама познат магазин који пише искључиво о слободном софтверу. Међутим, ту су неки други интернетски портали као што је ИНФО Онлине и Технографија који међу стандардним темама из свијета ИТ новитета пишу успут и о новитетима у линукс свијету. Од пројеката свакако можемо поменути БХЛД (енг. *Bosnian Linux Distro*), прву Босанску линукс дистрибуцију која је развијена још 2004. године на Електротехничком факултету у Сарајеву. Пројекат је имао неколико успјешних издања, али је изненада прекинут још 2011. године. Међу другим пројектима које можемо поменути је и

ДебКонф11, Дебијанов догађај који је био одржан у Бањој Луци од 24. до 30. јула 2011. године. Веома вриједан помена је и БарКамп, који се одржава на Електротехничком факултету у Бањој Луци и који већ четврти пут за двије године окупља велик број стручњака са занимљивим предавањима. Извештај са другог БарКампа је могуће прочитати у четрдесетом броју часописа или на сајту (https://libre.lugons.org/index.php/2015/11/izvestaj-sa-barkamp-konferencije-iz-banjaluke/).

Могла би се још поменути и модификована линукс дистрибуција за веб дизајн по имену Слобеликс 12 Веб Дизајн, пројекат тројице студената са Факултета за информационе технологије Универзитета у Бијељини. Како се наводи у званичном чланку о овом интересантном пројекту, Слобеликс је намијењен искључиво за веб дизајн, опремљен великим бројем алата отвореног кода као што је Аптана

Студио, те Блуфиш - намјењеним веб програмерима и дизајнерима.

Закључак

Слободан софтвер у Босни има велике потенцијале уколико се развије адекватна образовна стратегија која би искључила информатичку едукацију младих на рачунарима са комерцијалним софтвером, а више у фокус ставила обуку кориштења линукс дистрибуција и Либре Офиса који представља сјајан офис-пакет и тренутно најбољу бесплатну алтернативу комерцијалном Мајкрософт Офису. Наш образовни систем је такав да се линукс оперативни системи ријетко када могу видјети у сталним образовним програмима како наших школа, тако и техничких факултета. Такво стање линукс оперативног система на терену се правда тиме што је Виндоуз доминантна платформа, а више од 80 процената рачунала у Босни и Херцеговини их користи што у јавном, тако и у приватном сектору - док је линукс остављен по страни. Факултети и школе једноставно не пружају обуку кориштења линукс оперативних система, нити подстичу своје студенте и ученике на кориштење слободног софтвера. Срећом, постоје људи, студенти и ентузијасти у овој земљи који виде велику предност слободног софтвера те сами стичу вјештине у кориштењу, едукацији и промоцији линукса и филозофије слободног софтвера.

fedora 24

Аутор: Момчило Медић

Последње издање Гну-Линукс дистрибуције Федора доноси умерен број промена. Наиме, већина унапређења се односи на измене унутар система, док је број визуелних разлика прилично мали.

Гном је у верзији 3.20 и поклапа се са узводним издањем, а долази са новим приказом тастатурних пречица, унапређеном претрагом датотека, контролом медија у „календарском менију" као и побољшаним подешавањима за послове штампе и управљање мишем. Новина, која је кроз надоградње такође стигла и у претходну верзију (23), јесте и то да су системске надоградње на последње издање Федоре могуће и кроз графички интерфејс. Апликација Софтвер ће у

Представљамо

позадини преузети потребне датотеке и понудити вам поновно покретање система са надоградњом. По обичају мешање програма који не долазе уз дистрибуцију могу узроковати неочекиване последице. У том случају обратите додатну пажњу. У истом програму је уведена и подршка за Флатпакове, нови систем дистрибуције софтвера који би требало да обезбеди потпуно изоловано инсталирање и покретање програма.

Либре офис који стиже уз ово издање Федоре је верзије 5.1 и са собом доноси бројна побољшања у руковању Гнумерик, Микрософт.врри и Епл Кинот документима, као и извозу у ООХМЛ, МС Висио и Корел дроу форматима. Промена на ГТК+ 3 ће учинити да Либре офис изгледа још више као део система, а подршка за Вауланд је сада потпуно природна и спремна је за кориснике који су већ прешли на нови графички сервер. Када смо већ поменули Вауланд, потребно је додати да је сада спреман за свакодневну употребу и да се очекује да ће бити подразумевани графички сервер од следеће верзије Федоре.

Серверска едиција Федоре има нову шему партиционисања и сада није неопходно „заузети" сав простор на диску него се то може и накнадно урадити чак и помоћу графичког веб-алата Кокпит. Остале измене обухватају смањење заузетог простора при инсталацији изузимањем одређених пакета, као и ФрееИПА доменски контролер у верзији 4.3.

У настојању да Федора клауд постане најбоља платформа за контејнере, од сада је у дистрибуцији доступан и Опеншифт ориџин, систем заснован на Кубернетес који служи за оркестрацију контејнера.

Изведбе Федоре прате ново издање и пружају скуп програма и алата који треба да задовоље специфичне намене. Ако не желите да користите подразумевано Гном окружење и испробате нешто другачији изглед, а притом и даље користите познате алатке за управљање системом, онда су за вас доступне изведбе као што су КДЕ, Икс-еф-се-и (енг. *Xfce*), Синамон, ... Такође постоје и изведбе организоване око специфичних намена као што су музичко стваралаштво, роботика, играње, сигурност, научни рад и слично.

Већина просечних корисника неће приметити разлику између претходне и актуелне верзије Федоре, али то показује да измене које се уводе нису радикалне и не проузрокују узурпацију начина рада на који сте навилки. Такође, заједница никако није докона и константно ради на усавршавању система, унапређењу стабилности као и побољшању самих алата којим се одржавају инфраструктура и прави сама Федора.

Федора Србија заједница вас подсећа да сте сви добро дошли и цењени као сарадници. Без обзира на вашу стручност, професију, занимање или слободно време, свако од вас може да учини Пројекат бољим за све.

Како да...?

Нумеричка обрада и симулације
(7. део)

Аутор: Стефан Ножинић

Како се описују физички системи

Сваки физички систем има неки модел који га описује или апроксимира. Најједноставнији пример је падање лоптице на под. Ми знамо да на лоптицу делује гравитациона сила и на основу тога примењујемо други Њутнов закон. За дату лоптицу имамо једначину која нам описује колико у датом тренутку износи убрзање лоптице. Како наша лоптица има исто убрзање у сваком тренутку - гравитациона сила се не мења, што значи да се њена брзина мења линеарно (повећава се) а да се пређени пут може описати квадратном функцијом. Како ово знамо? Убрзање је промена брзине у јединици времена (извод брзине), а брзина је промена пређеног пута у јединици времена, односно убрзање је други извод пређеног пута. Како наш модел исказује колико је убрзање лоптице, ми морамо да то убрзање интегралимо два пута како бисмо добили пређени пут. Једначина која описује кретање лоптице је диференцијална једначина.

Заправо, сваки физички систем се може описати као диференцијална једначина.

Диференцијалне једначине првог реда

Овај тип је основни тип диференцијалне једначине. За дату функцију x (која може бити позиција или нешто друго) диференцијална једначина је:

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

Са леве стране нам се налази промена функције у зависности од промене времена, а са десне стране нам се налази вредност те промене.

Ојлеров метод за решавање диференцијалне једначине првог реда

Најједноставнији начин да решимо горе описани тип једначине је следећи:

Ако имамо вредност наше функције у неком тренутку и она износи $x(t)$, ми желимо да одредимо наредну вредност функције. Како су рачунари дискретне машине и не можемо превише ићи у детаље - не можемо одредити вредност функције баш у сваком тренутку. Оно шта можемо урадити јесте да израчунамо у приближном тренутку после Δt времена односно да одредимо

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

Ово можемо урадити баш захваљујући поставци наше једначине јер је:

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

Када ово средимо, имамо Ојлеров корак за наредни временски корак:

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

Диференцијалне једначине другог реда

Ово су сложеније једначине, али се врло лако пребацују на једначине првог реда. Оне су облика:

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

односно, може се и лакше записати као $x=f(t,x,x')$. Ако би нам x био пређени пут онда је x' брзина а x'' нам је убрзање.

Како ово решавамо? Уведемо смену $v=x'$ и онда имамо следећу ситуацију:
$v'=f(t,x,v)$ и $x'= v$

Прво решимо прву једначину помоћу Ојлеровог метода, а онда нову вредност за брзину убацимо у другу:

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

Како да...?

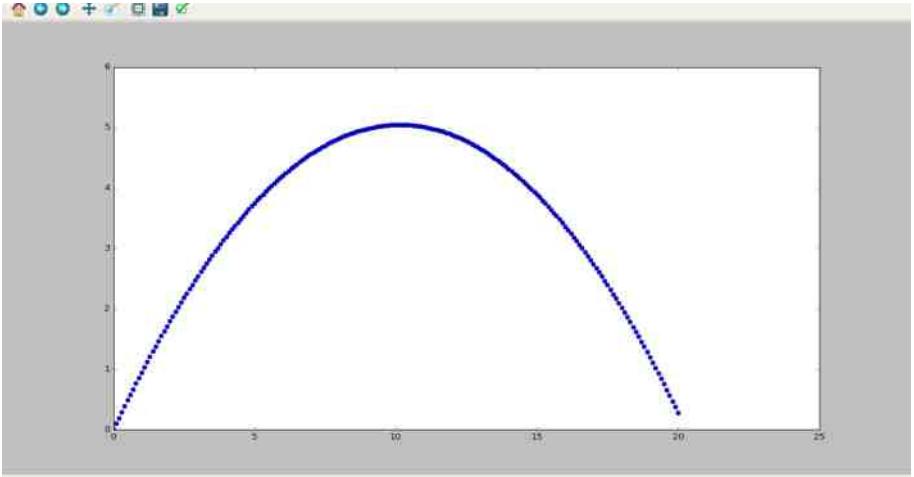
Пример - коси хитац

Ево и примера како бисмо урадили симулацију бацања лоптице укосо.

```
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()
```

Потребно је приметити да овде имамо две позиције, две координате пошто радимо у дводимензионалном систему. Код можемо и краће написати ако дефинишемо позицију и брзину као векторе.



```
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
```

Како да...?

```
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()
```

Додатни методи за нумеричко решавање диференцијалних једначина

Често Ојлеров метод није довољно стабилан или тачан. Због овога постоје и друге методе као што су Рунга-Кута и имплицитни методи. Предлажемо вам да пронађете на интернету како се они користе како не бисте долазили до проблема да вам Ојлер не решава проблем довољно стабилно или тачно.

КиПасИкс

Аутор: Марјан Ђуран

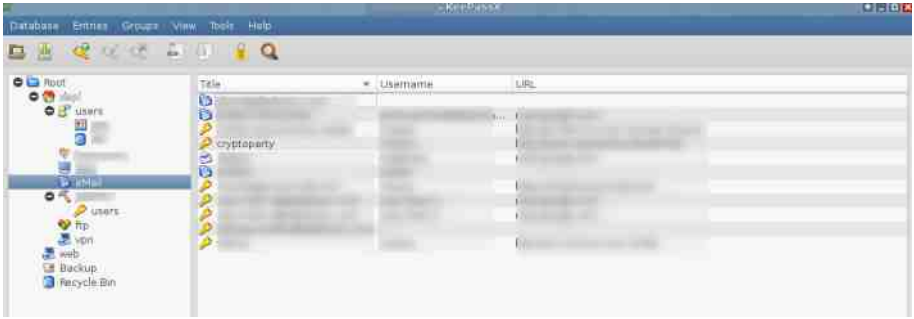
Зашто

Један од видова безбедности јесте шифра. Данас просечан корисник има минимално пет различитих налога: за мејл, омиљени форум, друштвену мрежу, онлајн продавницу и ко зна шта још, а све од наведеног може бити и у множини. Једини начин на који корисник може да утиче на безбедност свог налога јесте да има „добру" шифру (и да је редовно мења). Шта значи добра шифра? Више о шифрама могли сте чути и на Балкону (енг. *Balccon*) 2015. године (http://goo.gl/6PRv4H). Укратко, шифра не сме бити ништа смислено. Најједноставније речено, требало би да је насумично генерисан, што дужи низ што различитијих карактера. Ту се јавља неколико проблема, први је како генерисати? То је заправо најмањи проблем и може се решити на више начина. Можемо да искуцкамо жмурећи насумично по тастатури, генерисати хеш (енг. *hash*) било чега, користити *rand()* функције или програме за то намењене. Али проблем како тако насумично генерисану шифру упамтити, а како тек пет или више њих (добро је познато правило да се шифре не смеју записивати по цедуљицама), не може баш било која апликација да реши. КиПас је једна од ретких апликација која може да се похвали готово свим сегментима манипулисања и владања шифрама.

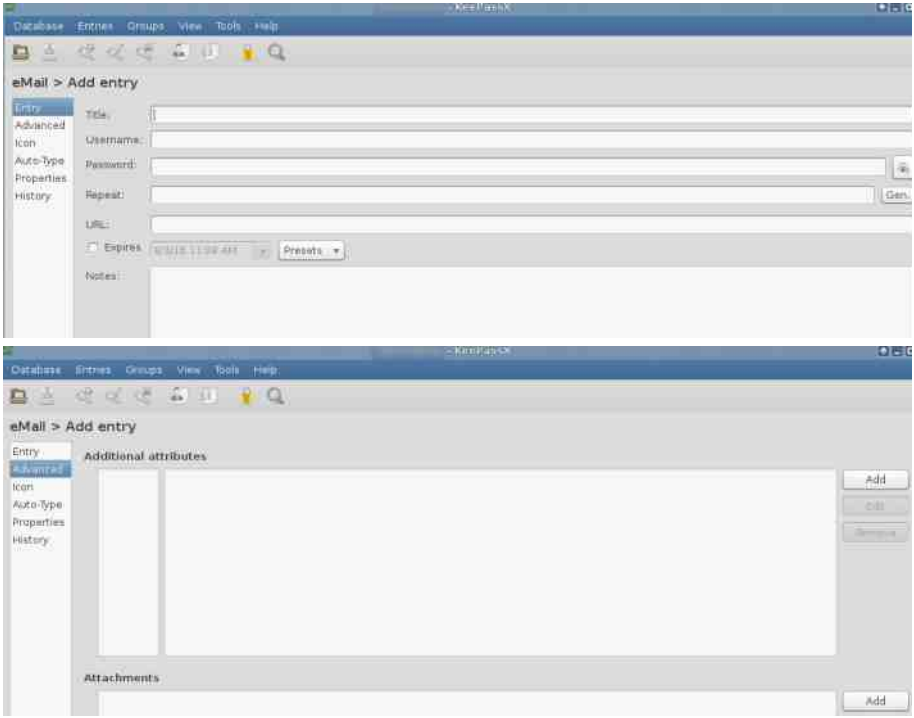
Шта је и кратак опис

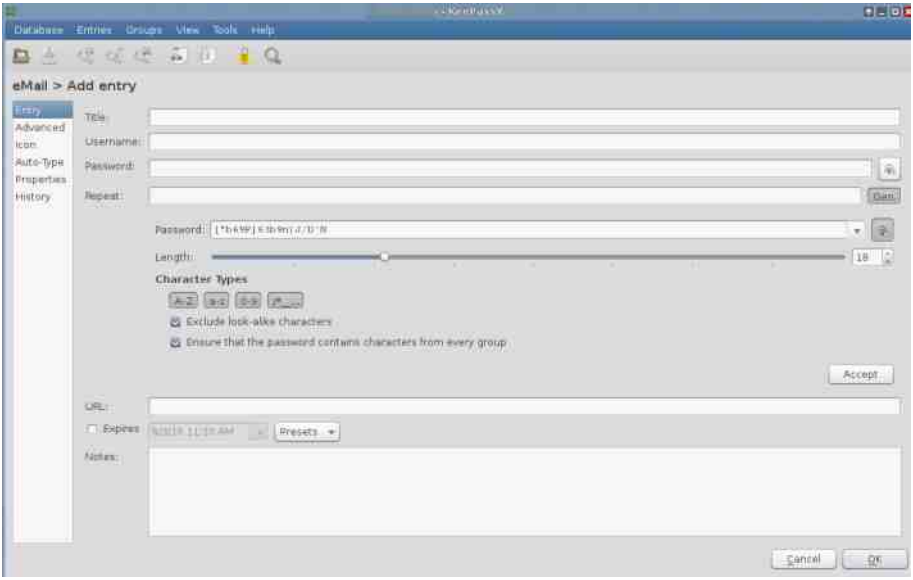
КиПас је апликација која служи за чување шифара, поред тога има могућност и генерисања шифара уз одабир карактера који ће учествовати и њиховог броја, све то уз прилично лепо организован графички интерфејс који је врло јасан и прегледан. У левом делу налазе се групе и подгрупе које можете сами креирати организовати, нпр. мејл, друштвене мреже, форуми... Док се са десне стране отвара списак креденцијала за одабрану групу или могућност за нови унос.

Како да...?



Све што у програму желите да урадите, можете на више начина, кроз тулбар (енг. *toolbar*), десним кликом или скраћеним путем, комбинацијом тастера на тастатури. Додатна могућност јесте да се уз сваки унос шифре, под опцијом „*Advanced*" дода и неки атрибут нпр. кратак опис који садржи одређени текст или чак прилог (енг. *attachment*), који ће такође бити шифровани.





Још једна од погодности је што КиПас можете, али не морате инсталирати. Дакле, можете да носите све своје креденцијале шифроване на УСБ флеш меморији. Постоји и могућност вишекорисничке употребе. У пракси то значи да базу можете држати на дељеном или мрежном диску, и да њој може приступати више људи. Постоји и могућност увожења из датотека *XML*, *CSV*, *TXT* екстензија.

Шта то издваја КиПас? Поред једноставности корисничког дела, КиПас издваја то што све шифре чува у интерној бази (коју корисник види као обичну датотеку) која је шифрована комбинацијом два алгоритма - AEC и Туфиш (енг. *Twofish*). На званичном сајту се посебно напомиње да нису само поља са шифрама енкриптована, већ цела база.

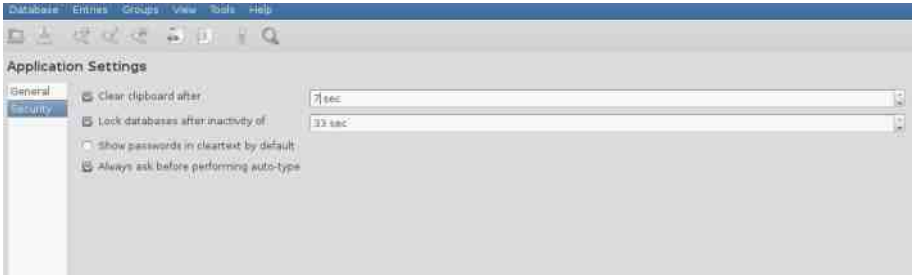
Мало криптографије

Кратак опис алгоритама који се користе. AEC (енг. *Advanced Ecryption Standard*) симетрични алгоритам који задовољава сигурносне захтеве у већини примена, до сада нису пронађени несигурни или потенцијално несигурни кључеви. Темељи се на Ријдил (енг. *RIJNDAEL*) алгоритму који је отпоран на линеарне и диференцијалне криптоанализе. Развили су га Јоан Даемен и Винсент Ријмен. Туфиш (енг Twofish) је тзв. AEC финалиста, симетричан блоковски алгоритам који

Како да...?

према ауторима нема слабих кључева, али има једноставан дизајн који олакшава анализу и имплементацију. Развијен је од стране компаније Кантерпејн системс (енг. *Counterpane Systems*), а аутори су Брус Шнајер, Џон Келсеј, Даг Вајтинг, Давид Вагнер, Крис Хал и Нилс Фергусон. Оба алгоритма шифрују блокове текста 128 бита, кључем дужине 256 бита.

Поред тога, главна шифра (енг. *master password*) се чува у облику CXA256 хеш (енг. *hash*) функције. Шта то значи? Хеш функција облика је **y=f(x)**, за неку датотеку било које величине или текст било које дужине карактера (x) добићемо хеш функцију (y) увек исте дужине. На пример, ако је претходна реченица улаз, излаз изгледа овако: **6205f2515ec0f62920d33759d31ee37eb5aa8d5da6b0370915b72349dfaa039a**. Једна од многобројних примена хеш функција јесте чување шифара на диску, па се тако и овде користи. Изабрана је хеш функција CXA256 (енг. *Secure Hash Algorithm 256*), 256 је дужина добијене функције, развијена је од стране НИСТ-а и НСА агенција. Пример CXA256 алгоритма http://goo.gl/piuL0k. Да се вратимо самој апликацији, једна од такође занимљивих могућности јесте да за базу не користите шифру, већ кључ (енг. *key file*). Иако на први поглед звучи као неки кључ који је потребно генерисати као за ССХ, у питању је заправо било која датотека. Дакле, можете користити филм, текст, слику... Ова опција је нарочито корисна уколико страхујете од килогера (енг. *key logger*), али се може користити и у комбинацији са шифром и тиме повећати ниво сигурности ваших шифара. Такође постоји и меморијска (енг. *In-Memory Streams*) заштита, што значи да се користи кључ сесије (енг. session key) док се учитава програм у меморију и да су шифре чак и тада безбедне, као и заштита од напада грубом силом (енг. *bruteforce attack*).



Кроз тулбар мени, у „*application settings*" менију, може се подесити време чишћења клипборда, односно, након колико времена ће се шифра или корисничко име које сте копирали из КиПас-а, обрисати и постати недоступна за

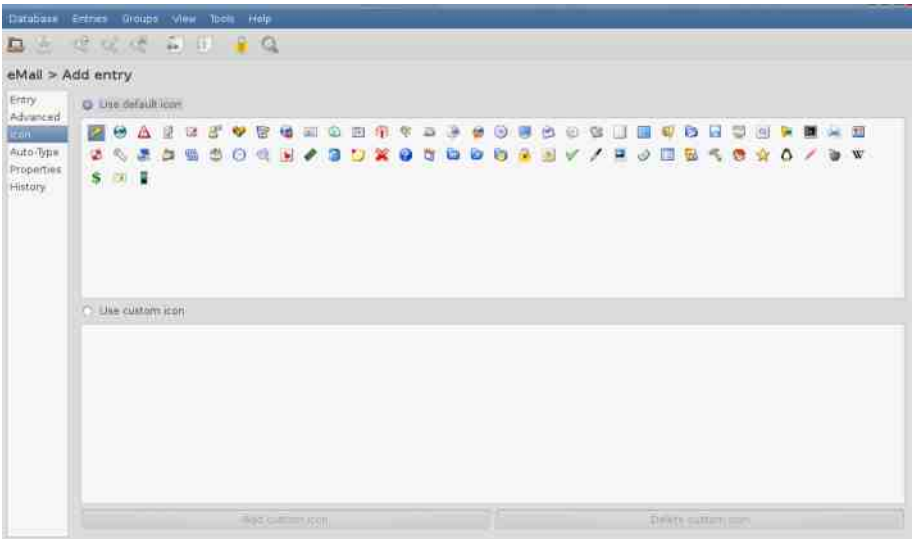
поновно налепљивање тј. пејстовање (енг. *paste*). Такође, може се подесити и време самозакључавања базе након одређеног времена неактивности, у случају да одете од рачунара, а оставите базу откључану.

Плугинови

Постоји доста плугинова за КиПас, све их можете наћи на http://goo.gl/jdOkm6, али овде су издвојена само три.

1. КиПасРФИД - додатак који омогућава дешифровање базе помоћу РФИД или НФЦ чипа посредством потребног хардвера, може бити одличан додатак безбедност ваше базе.
2. *QR* Kod Генератор - омогућава приказ шифре у облику QP кода, занимљив начин чувања шифре, замислите да носите налепницу са QR кодом на телефону, скенером на вашем рачунару откључавате КиПас базу!
3. *Application Icons* - КиПас има свој сет иконица, иако је могуће да сами увезете било коју другу (будите опрезни са увижењем иконица преузетих са интернета, претходно их проверите), овај плугин има свој сет нових иконица.

Како?



Како да...?

Кипасикс се налази на репозиторијумима готово свих дистрибуција, и можете га инсталирати једном командом.

Федора:

```
dnf install keepassx
```

Центос:

```
yum install keepassx
```

Арч:

```
pacman -S kepassx
```

Дебиан и деривати (Убунту, Минт, Кали):

```
apt-get install keepassx
```

На послетку, КиПас је (подразумевано) бесплатна апликација отвореног кода, доступна је за готово све платформе: линукс, Виндоуз, ОС Икс, Андроид, Виндоуз Фон, Ајфон, Хромбук, БлекБери, чак и за јава мобилне платформе (*J2ME*), Палм ОС, за веб-претраживаче постоји КиВеб, а за потребе оних који не воле графичко окружење или су из неког разлога спречени да користе ГУИ, ту је КПЦЛИ о којем ће бити речи у неком од наредних текстова.

За сада, КиПас има сам једну конкурентску апликацију, зове се Горила менаџер шифара, такође је отвореног кода, такође користи СХА256 алгоритам за хеширање главне шифре (енг. *master password*), такође користи Туфиш (енг. *Twofish*) алгоритам за шифровање базе (али само њега), и својим графичком интерфејсом доста личи на КиПас. Више о Горила апликацији можете видети на http://goo.gl/1436mh, а овде у неком од наредних текстова.

Како до сигурнијих шифара?

Аутор: Петар Симовић

Када помислимо о приватности наших података, прво што нам падне на памет требало би да је шифра. Зашто? Зато што се у суштини класично симетрично шифровање своди на шифру коју корисник унесе и податак на који се та шифра примењује употребом одређеног алгоритма коначан број пута. Погледајмо где се заправо данас све ослањамо на шифре како бисмо се заштитили од нападача и очували приватност. Најпре, сви користимо имејл, онда друштвене мреже попут Фејсбука и Твитера, затим, можда смо активни и на форумима или користимо неку од клауд услуга чувања података, ту је и приступ нашем рачунару или телефону, бежична (енг. *Wi-fi*) мрежа на коју смо повезани, и тако даље. Листа може бити оптерећујуће дугачка, и морате водити рачуна о свим тим шифрама за приступ одређеном налогу.

Ситуација у којој просечан корисник има више од десетак налога за које треба да памти шифре свакако представља проблем и води ка коришћењу једне шифре за све налоге, или употреби веома кратких и једноставних шифара. Штавише, корисници су често склони записивању шифара у једној незаштићеној текстуалној датотеци коју, да ствар буде гора, чувају на неком УСБ-у који даље прикључују на друге непроверене рачунаре. Чест је и случај да се шифре између корисника размењују путем незаштићених комуникација као што су имејлови, смс поруке, твитер или фејсбук директне поруке, па и слањем у облику текстуалне, људски читљиве, датотеке. Неретке су и ситуације у којима администратори или дизајнери неког мрежног сервиса или платформе погрешно рукују корисничким шифрама из незнања, недостатка новца или времена. Тако је чест случај да се шифре корисника на неком сајту чувају у текстуалној и људски читљивој датотеци тзв. плеинтексту (енг. *plain text*) или незаштићеној бази података, или се слање шифре између корисника и сервера не обавља преко заштићене везе тј. не користи се ССЛ.

Како да...?

Шта је сигурна шифра?

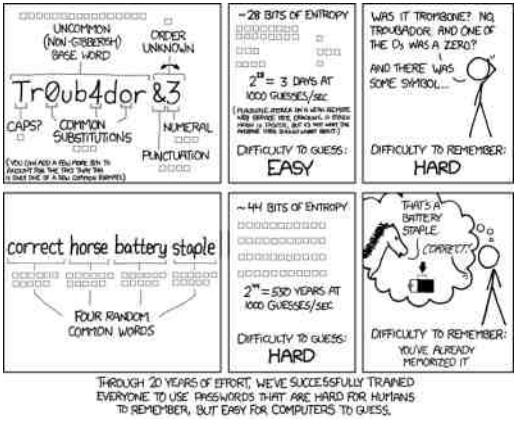
Како бисмо одговорили на ово питање, морамо прво знати како се мери сигурност шифре, тј. морамо увести појам **ентропије**. Ентропија је број битова који изражава колико је шифра јака поредећи је са одговарајућим низом насумичних битова. Тачна формула је једноставна и ако ентропију обележимо са E укључује дужину шифре D и скуп/сет могућих карактера из кога је шифра одабрана S**:**
$E = \log_2(S^D)$.

Примера ради, ако користимо само слова из азбуке (**S=30**) за састављање наше шифре, и ако нам је шифра дужине 8 слова/карактера (**D=8**), ентропија ће бити 39,25 (**$\log_2(30^8)$** https://goo.gl/vcAv) или око 4.9 бита ентропије по слову (ако се користе само мала или само велика слова). Наравно ентропија од 39,25 бита није довољна да заштити важне тајне. Препорука је да у зависности од врсте напада коју нападач изводи, ентропија буде већа (**80+ битова**) за офлајн нападе и (40+ битова) за мрежне нападе. Разлика је у томе што уколико нападач не може да дође у посед шифрованим датотекама или хешираној шифри, мораће да покушава да погоди вашу шифру директно на мрежи сервиса што је спорије и што се лакше уочава и спречава. Међутим, ентропија није најбоља мера, јер **комплексност** шифре није урачуната. Тако, на пример, наша шифра од 8 карактера могла је бити „лубеница" која није комплексна иако има сва различита слова. Ствар је у томе да је „лубеница" реч из речника и то је чини неотпорном на нападе речницима (енг. *dictionary attack*). Ту долазимо до још једног важног аспекта када је у питању начин на који корисници састављају своје шифре, а то је **насумичност**. Шифра „лубеница" није спој насумично одабраних слова азбуке, већ циљано бирана реч. Разна истраживања показују да су људи веома лоши у састављању насумичних шифара јер све раде по некој логици или обрасцу. Ни рачунари нису савршени извор насумичности, али са овог аспекта су бољи од људи. Зато је важно напоменути да је ентропија добар показатељ сигурности шифре ако се карактери бирају насумично, а не циљано. Ако користите енглески алфабет присутан на тастатурама, поред слова користите и бројеве и специјалне карактере „**0123456789**" (10 карактера) „**~`!@#$%^&*()_+-={}|[]\/;':"/.,?><**" (33 карактера) тј. све Аски (енг. *ASCII*) карактере који се могу одштампати. То је укупно 95 карактера (26 малих слова, 26 великих, 33 специјална карактера и 10 бројева). Скуп од 95 карактера вам даје и већу ентропију по карактеру, тј. имате око 6.5 бита ентропије по карактеру из овог скупа.

Поред шифара постоје и **фразе** (енг. *passphrase*) које у овом контексту означавају

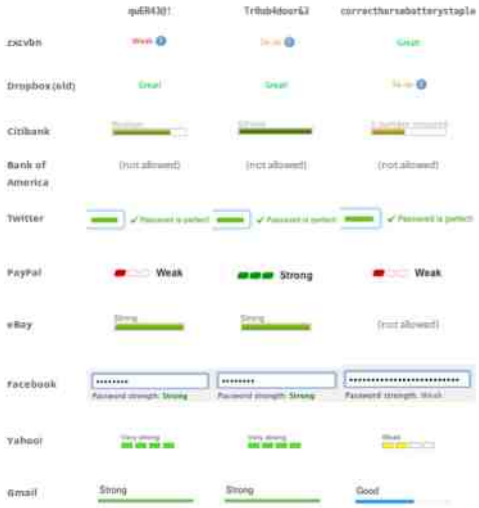
речи из речника. Наиме, уместо да користимо скуп слова из абуке или абецеде, користићемо речник као скуп познатих речи. Сигурно се питате „Речи из речника? А шта је са нападима речника". Одговор је заправо једноставан. Речник има много већи скуп елемената тј. речи него што азбука има слова, па је одабир пар речи бољи од одабира неколико карактера. Овај концепт се заснива на томе да је лакше упамтити 4 неповезане и насумично изабране речи из скупа од 7776 речи него 8 насумичних карактера из скупа од 95 ($\mathbf{\log_2(7776^4)=51;}$ $\mathbf{\log_2(95^8) = 52}$) за исту ентропију сигурне шифре.

Истакнимо још једном да је насумичност важно својство процеса генерисања сигурних шифара или фраза. Ентропија као мера сигурности шифре или фразе је тачнија ако се шифра саставља од насумично бираних карактера, односно фраза од насумично бираних речи из одређеног скупа. Међутим, насумичност је још важнија за одбрану од напада **социјалним инжењеригом** (енг. *Social Engineering*) о коме сте могли да прочитате у 39. броју. Како бисте избегли да нападач познајући вас, ваше навике и интересовања може лако да погоди вашу шифру, најбољи начин је да избор шифре или фразе препустите насумичности. Састављање сигурне фразе може бити и занимљиво или чак личити на дечју игру једноставном **дајсвер** (енг. *Diceware* https://goo.gl/oukz5n) методом. Узмите листу речи или речник (можете наћи и преузети са https://goo.gl/pXBYJL или https://goo.gl/AABLJE) и једну коцкицу. Затим баците пет пута коцкицу и запишите бројеве које добитете (на пример ако добијете 32512 тај број ће одговарати речи „*heat*" у листи https://goo.gl/ZUOLQW на страни 14.) Значи пет бацања коцкице вам даје једну реч, а треба вам најмање 4 речи за сигурност фразе од преко 50 битова ентропије.



Како да...?

Важна напомена је и да замењивање слова „A" са бројем „4" или карактером „@", или слово „O" са бројем „0" или карактером „*" неће унапредити сигурност шифре, већ ће вам само дати лажан осећај сигурности. Када нападач покуша да пробије неку шифру, он наравно зна за замене ове врсте и направиће програм који ће речи из речника пробати и заменом одређених карактера за бројеве. На пример шифра „*MyPassword123*" са заменама може да изгледа „*MyP@SSw0rd123*". Да ствари буду горе, по неискусне кориснике, када овакву шифру за замењеним карактерима испробате у неким од познатих онлајн мерача сигурних шифара, добићете задовољавајуће или чак одличне оцене јачине ваше шифре (резултате можете видети на: http://imgur.com/a/mjV4l). Док за исту шифру, други мерачи сигурности шифара дају реалније резултате (резулате можете видети на: http://imgur.com/a/Yla5t). Нису сви мерачи сигурности шифара исти.



Када смо већ код онлајн мерача сигурности шифре, будите веома опрезни. Иако већина тврди да не прикупљају ваше шифре које проверавате на тим сајтовима, такву тврдњу је тешко проверити. Зато саветујемо да **сами насумично генеришете и проверите сигурност ваше шифре без коришћења онлајн сајтова и програма.** Уколико вас мрзи да ручно рачунате ентропију ваше шифре, можете посетити https://goo.gl/9OyNMY сајт који вам неће тражити да унесете вашу шифру, већ податке о њој (да ли користите слова, бројеве специјалне карактере и које је дужине шифра).

Осим мрежних мерача сигурности и јачине шифара, на нету се могу лако наћи и гомиле правих корисничких шифара које су прибављене у разним неовлашћеним приступима сајтовима и њиховим базама података. Једна таква база података са шифрама је јавно доступна на гитхабу https://goo.gl/VCbGj9. А за више о најкоришћенијим шифрма посетите http://wpengine.com/unmasked/.

Када правите шифре или фразе, трудите се да имају 80 или више битова ентропије, да користите и мала и велика слова, бројеве и специјалне карактере насумично одабране. Фразе бирајте исто насумично из неког речника, одаберите да фраза има најмање четири насумичне речи. За сваки налог правите нову шифру/фразу, никако немојте употребљавати једну исту шифру/фразу за више налога, нови налог тотално нова независна шифра/фраза. Користите неки менаџер шифара (енг. *password manager*) отвореног кода. Никако немојте записивати шифре/фразе на папир, или их чувати у људски читљивој текстуалној датотеци.

Како сигурно чувати шифре?

Менаџери шифара

Просечан интернет корисник има више од 10 различитих налога (зависно од истраживања просечан број се креће од 17 до 27 https://goo.gl/oZ4B14, https://goo.gl/tzFzUQ). Тај број тачних шифара није лако памтити, а поготово може бити тешко запамтити која шифра је за који налог. Да би се обичном кориснику олакшао свакодневни живот, у сајбер свету постоје **менаџери шифара** (енг. *password manager*). Оно што је још важније, међу њима постоје и они који су отвореног кода. Менаџери шифара ће за ваш налог генерисати насумичну

шифру/фразу жељене дужине и сигурности, чувати је у шифрованој бази са осталим налозима. База свих ваших налога се шифрује једном шифром коју морате запамтити. Предност менаџера шифара је у томе што памтите једну шифру уместо за сваки налог посебно. Препоручујемо Кипасикс (енг. *KeePassX*, https://www.keepassx.org/) или Кипас (енг. *KeePass*, http://keepass.info/) који постоји за Мек о.с. (енг. *Mac OS*), Виндоуз (енг. *Windows*) и линукс, а постоји и Кипасдроид (енг. *KeePassDroid*, http://www.keepassdroid.com/) форк Кипас-а за андроид. За остале менаџере шифара можете посетити странице: https://goo.gl/XwKkJR или нашу скромну листу мање познати менаџера: https://goo.gl/pPUcjj). Постоје и групни менаџери шифара као што су Тимпас (енг. *TeamPass*, http://teampass.net/) и Пасболт (енг. *Passbolt*, https://www.passbolt.com/) Када користите било који менаџер шифара, направите бекап шифроване базе на неком спољном сигурном медијуму који нећете давати свима.

Постоје и мрежни менаџери шифара који шифровану базу шифара синхронизују са неким мрежним сервером. На тај начин уколико изгубите свој уређај на коме сте држали шифре, и даље можете приступити вашим шифрама складиштеним на серверу. Редунданса свих ваших шифара је заиста неопходна, поготово ако нисте добри у памћењу шифара. Ово ипак може представљати ризик по сигурност ваших шифара јер поред сигурности вашег уређаја, од велике важности је и начин комуникације са сервером, сама безбедност сервера, као и јачина шифре којом сте шифровали базу шифара пре слања на сервер. Такав је рецимо Енкриптер (енг. *Encryptr*, https://goo.gl/HdaeQR).

Мане менаџера шифара

Евентуалне мане коришћења менаџера шифара представља централизовано место које садржи све ваше шифре, па тиме представља мету евентуалних нападача/хакера. Затим прављење резервне копије и чување исте на довољно безбедном месту, као и евентуални пропуст у самом програму, може имати негативан ефекат на сигурност корисникових шифара. Напоменимо и то да је од

великог значаја који криптографски алгоритми се користе за шифровање базе шифара унутар менаџера, као и која се хеш (енг. *hash*) функција користи за чување главне шифре. Јер нису сви криптографски алгоритми сигурни (РЦ4 и ДЕС, https://goo.gl/V8qD3h), као што ни све хеш функције нису сигурне (МД2 и МД4 и МД5, РИПЕМД, https://goo.gl/LKzsDI).

Алтернативе менаџерима шифара

Да ли морате да чувате шифре уопште? Да ли постоји начин да памтите само једну сигурну шифру и да на основу ње креирате остале, без складиштења било које шифре на било ком рачунару или уређају? Овако нешто је заправо могуће, штавише веома просто. И ако сте помислили да на једну шифру само надовезујете по неки додатни карактер (пример: *tajna_šifra123*, *tajna_šifra1234*), нисте погодили, али били сте близу.

Концепт је следећи:

1. Саставите веома добру шифру или фразу са најмање 80 битова ентропије (пример шифре: **p:<(ZAS2O#PM** или фразе: **dim livada mačka sir crveno prozor)**
2. Одредите име апликације или сајта за који састављате шифру (пример за сајт **libre.lugons.org**).
3. Одредите хеш алгоритме које користите за састављање и евентуално дужину шифре (пример користићемо *base64*, *sha1*, и *sha256*)

Сада можете генерисати шифру из терминала по принципу:
echo "šifra/fraza:ime_aplikacije/sajta" | base64 | sha1sum | sha256sum

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

или

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

Што ће вам у првом случају дати **29a6eac9c1a6800a886fdbdb7f8a2a36b4fc55994728ab9b37bdb01a7f1da107**, а у другом **29a6eac9c1a6800a886fdbdb7f8a2a36b4fc55994728ab9b37bdb01a7f1da107**. Овај низ од 64 хексадекадна карактера можете једноставно смањити на жељену дужину додајући на крај претходних команди **tail -c 14** или **head -c 10** (што ће приказати последњих 10 или првих 10 хедксадекадних карактера).

Како да...?

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

Програми који ово раде постоје и то су Мастер пасворд (енг. *Master Password*, https://goo.gl/R6t2BI GPLv3), пвдхеш (енг. *PwdHash*, https://goo.gl/jagYyt) и СуперГенПас (енг. *SuperGenPass*, https://goo.gl/4PtFO0 GPLv2). Сви су отвореног кода, а Мастер пасворд и СуперГенПас су доступни и као андроид и Ајос (енг. *IOS*), веб-апликације, С програм, и друге платформе (https://goo.gl/rQTCPX).

Овај систем генерисања и чувања шифара има предности када је реч о складиштењу шифара, јер оно не постоји. Ако вам неко украде рачунар, на њему се не налазе ваше шифре уопште. Уколико неко сазна шифру за један налог, помоћу ње не може сазнати остале шифре, овако генерисане, као ни главну шифру од које се све остале праве све док користите сигурне хеш алгоритме. Напомена је да погледате који су хеш алгоритми сигурни (https://goo.gl/LKzsDI), као и да не користите само base64 кодирање, наведено у претходном примеру, (ако не знате шта радите) јер *base64* није хеш функција и лако се може декодирати . У наведеном примеру base64 се ипак користи, али после њега се примењују две довољно сигурне и иреверзибилне хеш функције. Савет је да за хеш функције користите *SHA256*, *SHA512*, прихватљиве су и *SHA1*, РИПЕМД160 и Вирпул (енг. *Whirpool*) доступни унутар ОпенССЛ-а, а ако сте прави параноик користите БЛАКЕ2 (https://blake2.net/), али по цену удобности и преносивости. Врло је важно одабрати добру главну шифру, као и сигурне хеш алгоритме, јер од њих зависи сигурност свих ваших шифара генерисаних на овај начин. Наравно, постоје одређене мане углавном везане за мењање већ постојећих шифара, јер захтева памћење још једаног податка (да корисник памти и број колико пута је променио шифру за одређени сајт) што може бити веома незгодно са порастом броја налога који активно користите. У том случају би алгоритам изгледао отприлике овако:

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

Друга мана је што ћете морати брзо променити све шифре уколико нападач сазна вашу главну шифру. Приметите да начин на који генеришете шифре није тајна, и нападачу неће значити много информација које хеш алгоритме користите док год су они сигурни, и док год је ваша главна шифра довољно компликована.

Генератори шифара и фраза

Поменућемо да за линукс постоје веома корисни ЦЛИ програми попут пвген-а (енг. *pwgen*) који вам помаже да генеришете насумичне шифре (кога када инсталирате можете користити рецимо овако: **pwgen -sy 20 15** и који ће вам понудити 15 различитих, независних и насумичних шифара, где је свака шифра дужине 20 из скупа од 95 карактера). Ту је и пасворд гнератор (енг. *password-generator*, https://goo.gl/Suigwo) који може генерисати шифре које се лако памте

```
password-generator -l 20
```

Или једноставније, без инсталирања додатних програма

```
openssl rand -base64 20
```

или

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

За генерисање фраза можете користити Икс-кеј-Си-ди-пас (енг. *xkcdpass*, https://goo.gl/d8TJrB) и добити лако памтљиве фразе попут ове:

```
Yeti permutes kilobyte visa string
```

Закључак

Како ћете генерисати и где ћете чувати шифре је свакако на вама. Употреба сигурних шифара није тешка, и програми попут Кипас-а и СуперГенПас-а то олакшавају максимално. Свакако се исплати мало се потрудити око својих шифара, не зато што нешто кријемо, већ да нас не би болела глава када неки хакер провали тајну шифру „**password1234**".

Ослобађање

Наредбе у Гну-Линуксу

(2. дио)

Аутор: Адријан Ђурин

Након вишегодишњег коришћења наредби из првог дијела овог серијала чланака, крајње је вријеме да се науче нове наредбе. Кретање кроз директорије (**cd**) и излиставање њиховог садржаја (**ls**) се јако често користе, а понављање је мајка знања - а и од главе вишак не боли. У наставку чланка позабавит ћемо се стварањем. Јер, тко не воли стварати? Креирати празан фајл може се на више начина, а један од њих је наредбом **touch**.

Ако се налазимо у директоријуму у којем желимо креирати празан фајл, то радимо наредбом **touch <име_фајла>**. Например, желимо креирати попис ствари које желимо купити у мјесној продаваоници свега и свачега:

```
touch veoma_lijep_popis.txt
```

Наредбом за излиставање **ls** можемо провјерити постојање фајла. Фајл је празан и спреман да у њега упишемо све жеље и захтјеве - уз цијене, наравно. Како бисмо уписали било што у тај фајл, морамо се послужити новом наредбом. Нано представља веома једноставан уређивач текста унутар љуске линукс система. Доступан је на великој већини дистрибуција.

```
nano veoma_lijep_popis.txt
```

Извршавањем те наредбе отвара нам се једноставно сучеље. Уписивање се врши типковницом, и уз мало труда ваш попис може изгледати као на слици.

[1] – име фајла [2] – попис [3] – keyboard shortcuts, јер нема алатне траке

Како бисте брзо провјерили што се налази у вашем текст-фајлу, а да притом не покрећете Нано, упишите:

```
cat veoma_lijep_popis.txt
```

Резултат је испис вашег текст-фајла у терминалу. Наредба cat има и неке друге посебности и разлоге кориштења, али о томе у каснијим чланцима.

Фајлови и директорији чине окосницу линукс сустава. Креирање директорија такође није претјерано тешко. Постоји наредба за то. Покушајте сљедећу:

```
mkdir igrice
```

Након тога излистајте све у тренутном директорију. Поред свих стандардних директорија, и пријашњег фајла, појавио се и нови директорij назива „igrice”. Можете се пребацити у њега помоћу наредбе cd да потврдите да се ради о директорију - додуше, празном директорију.

Ослобађање

Наредба

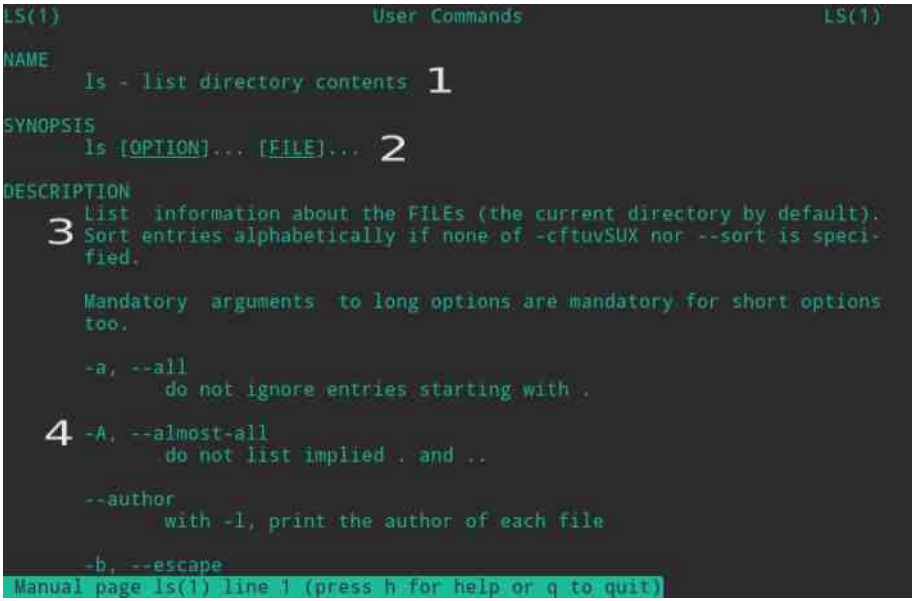
```
cd ..
```

вас враћа у претходни директориј.

Уколико нисте сигурни што чинити, **man** наредба је заправо *f1/help/malo_slabiji_google* за све што требате знати о појединим наредбама. Она је приручник у којем се налазе упутства за употребу наредби: што значи наредба, што ради и како се користи.

```
man ls
```

Ова наредба ће нам отворити приручник о **ls** наредби, што можете видјети на слици.



[1] – име наредбе [2] – како се користи [3] – опис наредбе [4] – додатни аргуметни (о томе у даљњим чланцима)

Кроз сучеље приручника се крећете или стрелицама горе/доље по један редак,

или типкама f и b по цијелу картицу. За излазак из приручника користи се типка q. Испробајте ову наредбу и са осталим наредбама које сте досад користили. Наравно, ако **man** не може помоћи онда врло вјероватно може Гугл.

У овом кратком тексту обрађене су наредбе које су везане за креирање фајлова (**touch**) и директорија (**mkdir**), једноставну обраду текста (**nano**) и наредбе која нам служи као приручник уколико заборавимо синтаску/сврху одређених наредби (**man**).

И, за крај, ево неколико наредби да се мало забавите и размислите. Што се догађа кад унесете сљедеће наредбе:

```
nano neki_drugi_popis.txt
man man
mkdir Moje pjesme
```

Преглед популарности Гну-Линукс и БСД дистрибуција у последњих шест месеци

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=

Пад <
Пораст >
Исти рејтинг =
(Коришћени подаци са Дистровоча)

Ослобађање

Нови живот старог рачунара

Аутор: Игор Стоиљковић

Јесте ли икада помислили шта бисте све могли урадити са старим компјутером чија је прва младост давно прошла? Бацити га? Да је тако не бисмо писали овај текст. Поклонити га старијим или млађим генерацијама у вашој породици/фамилији? Е то је већ нешто и има неке везе са овим текстом. Зашто се, уз мало уложеног труда, не бисте решили вашег старог рачунара (у неку руку) и подарили вашем детету или већ некоме другоме коме ће први информатичарски кораци можда променити живот?

Нормална је човекова особина да тежи ефикасности и управо том чињеницом можемо објаснити напредак човечанства; од простих секира и ножева од камена до нуклеарне фузије, мобилних телефона јачих од суперкомпјутера осамдесетих година и Трикордера. За аутора овог текста, симбол ефикасности је трансформатор јер је то најефикаснија машина на планети са степеном корисног искоришћења до 98%.

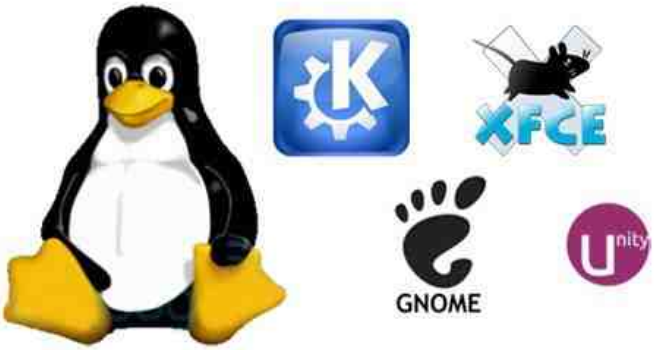
Бацање ствари које још раде и које могу да се користе у неку сврху није ефикасано понашање и требало би да се суздржимо од таквог понашања. Ипак, живимо у Србији, земљи чији су грађани преживели разне пошасти током година, од санкција, ратова и инфлације до „скорашње" транзиције. Могли бисмо да се угледамо на тај запад и по томе што ћемо искористити сваки доступан ресурс (ефикасност) а не само да постајемо конзумерско друштво попут њих јер оно су они а ми смо ми, са свиме што то носи.

Но, вратимо се ми на искоришћење (старијег) ресурса. Ако поседујете рачунар који има било који процесор са два језгра, 1 GB RAM меморије, било коју графичку карту и 20 GB простора на хард диску ви већ имате солидно јак компјутер и стога прилично велики избор дистрибуција које можете инсталирати на свој кућни

рачунар. Практично могу све али неће све бити са задовољавајућом одзивношћу и брзином. Неке дистрибуције могу радити већ са процесором од 500 MHz и већ са мање од 128 MB радне меморије, али аутор текста вам не препоручује мање од 512 MB ако баш не морате јер ипак не причамо о компјутерима из доста старијег периода и задовољство коришћења таквог система је дискутабилно (прим.аут.).

За почетак треба погледати какав хардвер имамо на располагању. Затим се распитати о дистрибуцијама и одабрати једну или више које вам делују као добар избор. Паметна је идеја пробати у живој варијанти све дистрибуције које то подржавају, а то је данас скоро свака. Треба водити рачуна и о „укусима", тј. о радним окружењима (енг. *desktop environment*) и управљачима прозора (енг. *window manager*). Не троше сви ресурсе на исти начин, и док су неки прелепи и крцати украсима, такви су „тежи" за систем (енг. *eye candy*), неки други су рудиментални али веома брзи и употребљиви.

Пример првих, лепих и гладнијих за ресурсима, били би Ка-Де-Е (енг. *K Desktop Environment*) и Јунити (енг. *Unity* - Убунтуово окружење), и донекле Синамон (енг. *Cinnamon*) и Мате (енг. *MATE*), мада су они пуно лакши од првопоменутог двојца. Једноставнији а бржи су Икс-Еф-Це-Е (енг. *XFCE*), Ел-Икс-Де-Е (енг. *LXDE*), Енлајтенмент (енг. *Enlightenment*), Оупен-бокс (енг. *OpenBox*), Флуксбокс (енг. *Fluxbox*) и *JWM* који је вероватно најбржи представник ове групе.



По ауторовом мишљењу, незахвално је убеђивати вас да узмете ову или ону дистрибуцију јер је то ствар личних преференција и афинитета, и то што некоме одговара нека дистрибуција не значи да ће се и вама свидети или вам одговарати. Ипак, аутор лично користи Мањаро линукс (енг. *Manjaro*) и прилично је задовољан њиме. За оне са јачим хардвером који воле лепо окружење је

Ослобађање

препорука Ка-Де-Е са Плазма (енг. *Plasma*) окружењем верзије 5. За оне са слабијим хардвером је препорука Икс-Еф-Це-Е (енг. *XFCE*), Оупенбокс или Флуксбокс.

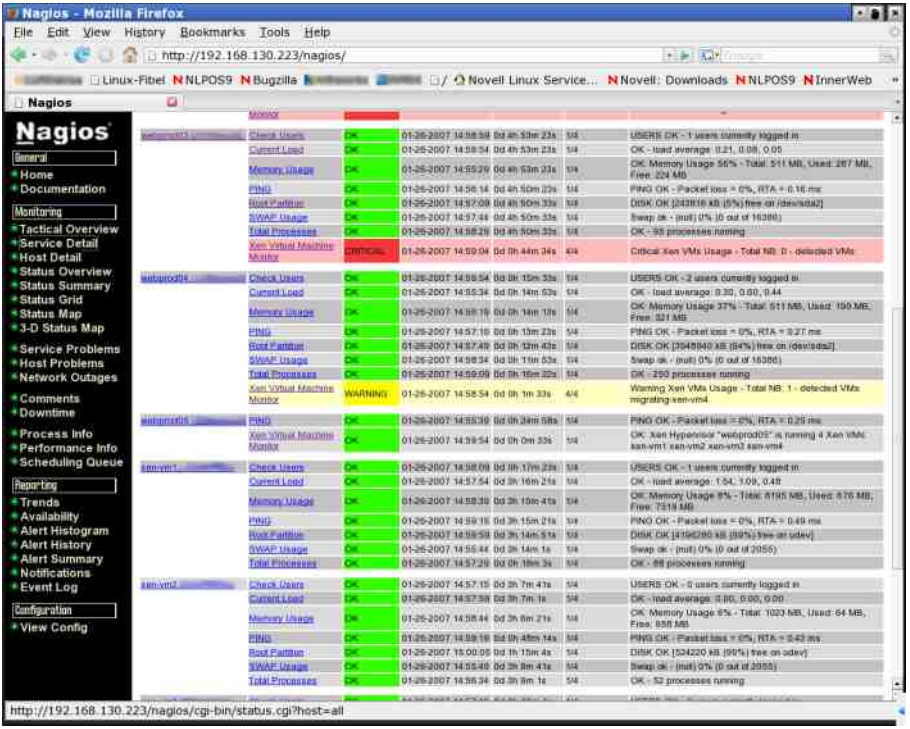
У суштини, ако вам се не свиди Мањаро изаберите дистрибуцију која вама одговара али се придржавајте правила о снази хардвера наведеној за Мањаро. Уживајте у свом новом старом рачунару.

ФАН

Систем за надзор сервиса и уређаја

Аутор: Стефан Бишевац

Ако се бавите системском или мрежном администрацијом, а дуго трагате за некомерцијалним решењем за надзор и аутоматизовани опоравак ваше мрежне инфраструктуре, онда ће вам овај текст дефинитивно олакшати у одлуци за имплементацијом једног од најкоришћенијих решења отвореног кода за мониторинг рачунарске мреже – Нагиос.



Слободни професионалац

Нагиос је већ дуго комерцијалан производ који нимало није јефтин за мала и средња предузећа, међутим, из жеље да остане у категорији решења отвореног кода, на званичном сајту Нагиос пројекта наћи ћете такозвани Нагиос Кор пакет који је потпуно бесплатан. У овом пакету садржани су општи фајлови за конфигурацију датотека, скромна база додатака и веб страница која илуструје статус надгледане инфраструктуре. Ако сте почетник и не познајете сасвим добро начин функционисања система за надзор сервиса, онда је најбоље да посетите овај сајт и тамо пронађете бесплатне Нагиос књиге који детаљно описују Нагиос Кор структуру. Нагиос је пакет који се инсталира на једној од линукс дистрибуција (најчешће на оној дистрибуцији којом добро владате). ЦентОС је постао стандард и омиљена дистрибуција многих системских администратора па је можда добро решење да Нагиос управо подигнете на ЦентОС-у због веома богате подршке за ову дистрибуцију.

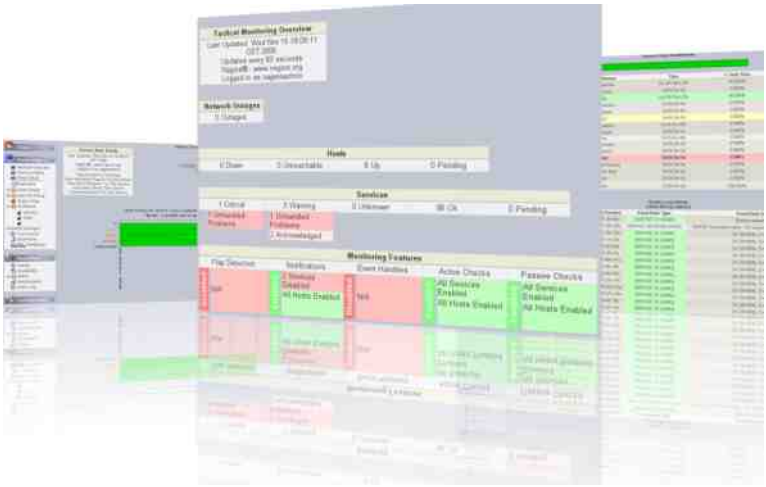
Ако сте до сада ипак имали прилике да радите са Нагиос Кором онда сигурно знате колико је напорно дефинисање нових рачунара, нових сервиса и нових команди јер се све ради из конзоле, а Нагиос фајлови умеју да буду преобимни па вам је за добру конфигурацију некада потребна изузетна концетрација. Нагиос фајлови су међусобно повезани па је и за уочавање најситнијих грешака некада потребно много времена. Најчешће грешке јављају се у некој стандардној програмерској форми, било да је то затворена витичаста заграда или изостанак неког слова у самој скрипти.

Нагиос XI је комерцијално решење Нагиос пројекта које садржи у себи веб страницу за графичко подешавање система за надзор. Статистика говори да је на овај начин знатно олакшан посао администраторима у конфигурацији и подешавању свих мрежних субјеката, чиме се максимално избегавају грешке у синтакси па се администратор много више посвећује суштинској конфигурацији ради што бољег подешавања Нагиоса за надзор свих делова мреже.

Претходна дистрибуција Нагиоса је комерцијална и веома скупа, међутим, група ентузијаста из Француске, а сада и из целог света, ради на пројекту ФАН (енг. *Fully Automated Nagios*). ФАН је замена за Нагиос XI, и према искуству системских инжењера, ФАН нимало не заостаје за Нагиос XI дистрибуцијом. ФАН долази у облику аплајенса и могуће га је потпуно бесплатно преузети са ове странице. Он у себи садржи 3 независна пројекта: Нагиос Кор, Центреон и НагВис.

- Нагиос Кор је срце овог система. Задужен је за обраду свих информација и

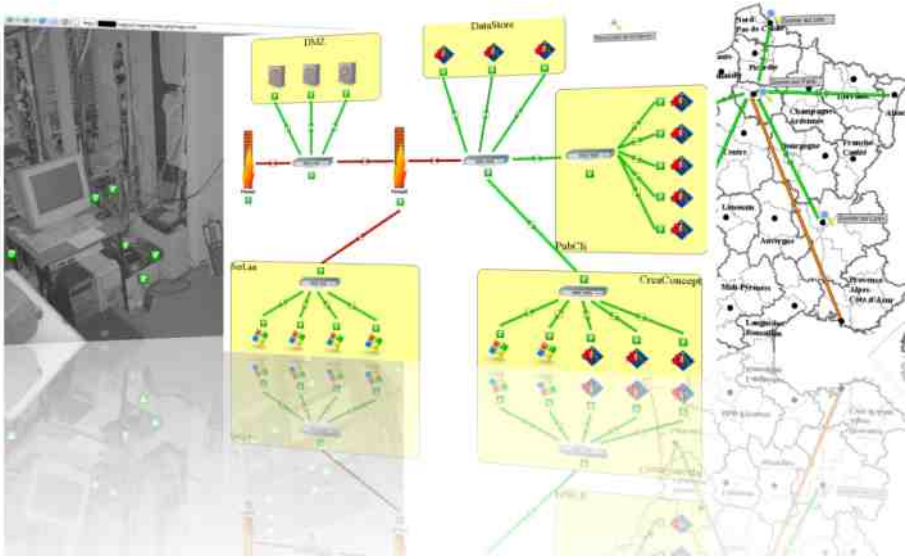
обавештавање администратора о проблемима у мрежи. Уколико искористите и његов ивент хендлер онда добијате потпуно моћан систем надзора који може сам да одлучује у одређеним ситуацијама.



- Центреон, снажан систем конфигурације који се јавља у виду веб окружења. Знатно олакшава посао уношења нових субјеката у систем за надзор или модификацију постојећих.

Слободни професионалац

- НагВис, представља систем за визуелизацију података. Уколико у вашој организацији постоји велики панел или ТВ на којем пратите стање сервиса, тада вам НагВис може много јасније показати шему ваше инфраструктуре на којима се налазе сервиси које сами дефинишете.



Уколико се још увек размишљате око система за надзор, тада је наша топла препорука да што пре зароните у свет линукса и Нагиоса и за вашу организацију успоставите снажан систем надзора и аутоматизованог опоравка критичних сервиса.

Ако немате стрпљења да читате обимне књиге на енглеском језику, онда пратите ЛиБРЕ! страницу јер ћемо у наредним чланцима објаснити детаљније сваки од делова ФАН пројекта понаособ, са осврtом на битне чињенице које би требало знати када је надзор рачунарске инфраструктуре у питању.

Крипто-ратови (2. део):
Некада и сада

Аутор: Петар Симовић

Клипер чип

Америчка национална сигурносна агенција (NCA) се није зауставила само на слабљењу софтвера, него је прешла и на хардвер, тачније чипове и процесоре. Ово је и разумљиво јер су прву битку за софтвер и алгоритме свакако добили активисти и сајберпанкери, а производња хардверских компоненти неопходних за генерисање криптографских кључева је била у власништву великих компанија подложних утицају државе и тајних служби.

Клипер чип (енг. *Clipper Chip*) је био пројекат NCA агенције деведесетих година прошлог века са циљем да се у мобилне телефоне угради чип намењен за шифровање звучне комуникације. Проблем је у томе што би тајни кључ одређивао произвођач чипа и тајно га прослеђивао NCA агенцији која је и дизајнирала алгоритам по коме би радио Клипер чип и који је такође био тајна. На овај начин NCA би без икаквог труда једноставно дешифровала сву телефонску шифровану комуникацију јер је знала тајне кључеве сваког уређаја. Влада је у сарадњи са

НСА агенцијом покушала да примора све телефонске компаније да угради овај чип у своје телефоне, али то није успело. Такође, Мат Блејз (енг. *Matt Blaze*) је успео да провали и заобиђе овај систем 1994. године. Ако овде застанемо јер је већ почео двадесет и први век, можемо рећи да су прве крипто-битке добијене, али ратови се настављају и даље, само мало неприметније. НСА је наставила да обогаљује криптографске протоколе и уграђује специјалне чипове у хардвер.

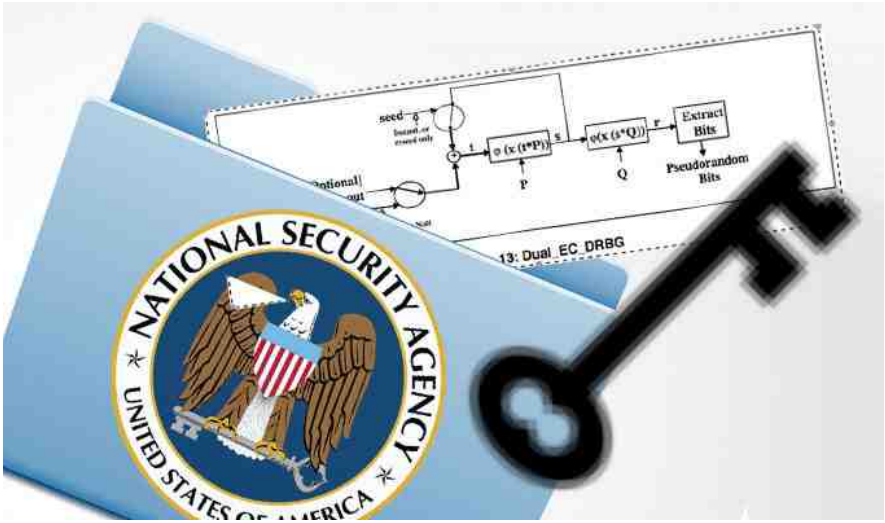
RdRand

НСА је касније подривала сигурност криптографије на нижим нивоима. Већина софтвера која је имплементирала неку криптографију је била отвореног кода и доступна за проверу свакога ко је то желео да уради. Такав пример је рецимо *OpenSSL* који имплементира најјачу познату криптографију и масовно се користи на серверима за сигурну комуникацију коришћењем симетричног, асиметричног шифровања и криптографских хеш (енг. *Hash*) алгоритама за аутентификацију. Оупн-Ес-Ес-Ел се ослања на друге системске програме за генерисање „насумичних" бројева који су потребни за прављење сигурних тајних кључева, а баш то је и место које је НСА напала како би овај протокол учинила мање сигурним. Ради се о генератору насумичности (*Rd_Rand*, https://en.wikipedia.org/wiki/RdRand) унутар Интелових процесора који враћа псеудослучајне бројеве, а за кога је почело да се сумња од 2013. године да је модификован како не би враћао „насумичне" бројеве, већ бројеве који се могу лакше предвидети. Ова тема створила је поделу и унутар Линукс заједнице јер је Линус Торвалдс одбацио сумње у нарушавање безбедности, док је Фри-Би-Ес-Ди престао да користи сумњиви генератор у језгру свог оперативног система (извори: https://goo.gl/LjHNYV, https://goo.gl/WsBHg3)

Dual_EC_DRBG

Када смо већ код генератора „насумичних" бројева, *Dual_EC_DRBG* је алгоритам за креирање „насумичних" бројева за елиптичке криве (енг. *Elliptic Curves*). Елиптичке криве се користе за генерисање асиметричних кључева исте сигурности али мање величине него *RSA*, и данас су најзаступљеније за успостављење сигурне комуникације на интернету, тј. унутар *HTTPS* протокола који свакодневно користимо. Као што можете претпоставити, овај алгоритам (*Dual_EC_DRBG*) је конструисала НСА и предложила га Америчком Националном институту за стандарде и технологију (енг. *National Institute of Standards and*

Technology, *NIST*), који бива усвојен и од овог института и од других релевантних сигурносних компанија као сигуран алгоритам. Наравно, од самог појављивања овог сумњивог алгоритма, објављиване су бројне публикације које су указивале да је алгоритам несигуран и то вероватно намерно бекдорован (енг. *Backdoor*) (https://goo.gl/vQuHLL, http://goo.gl/8EJp12). Несигурност алгоритма је потврђена и документима које је Едвард Сноуден (енг. *Edward Snowden*) изнео у јавност и који су објављени 2013. године кроз тајни програм под кодним називом Булран (енг. *Bullrun*) озлоглашене НСА. Булран је само један у низу оваквих тајних програма који спроводи НСА како би на све начине слабила и дешифровала сву заштићену комуникацију фајловима (https://goo.gl/aauXwb). Прошле године је објављено да је *Dual_EC_DRBG* био такође присутан у СкринОС (енг. *ScreenOS*) оперативном систему (енг. *firmware*) популарног фајрвола (енг. *firewall*) система НетСкрин (енг. *NetScreen*) (https://en.wikipedia.org/wiki/Dual_EC_DRBG#cite_note-54)



У документима које је Сноуден изнео у јавност, путем разних медија и Викиликса, види се да је НСА наставила да уграђује хардверске импланте у матичне плоче сервера, у-ес-бе-ова и других каблова. Да ствар буде гора, ово су радили пресрећући пошиљке намењене одређеним особама са купљеним исправним хардвером у које су на тајним локацијама уграђивали и подметали своје импланте. Ово је лепо документовано следећим видео материјалима господина Апелбаума (енг. *Jacob Appelbaum*) са једне ЦЦЦ конференције: https://goo.gl/GwC8s9 и https://goo.gl/Ymv2Gb.

Мобилни кутак

Шифровање електронске поште на Андроиду:

K-9 и АГП

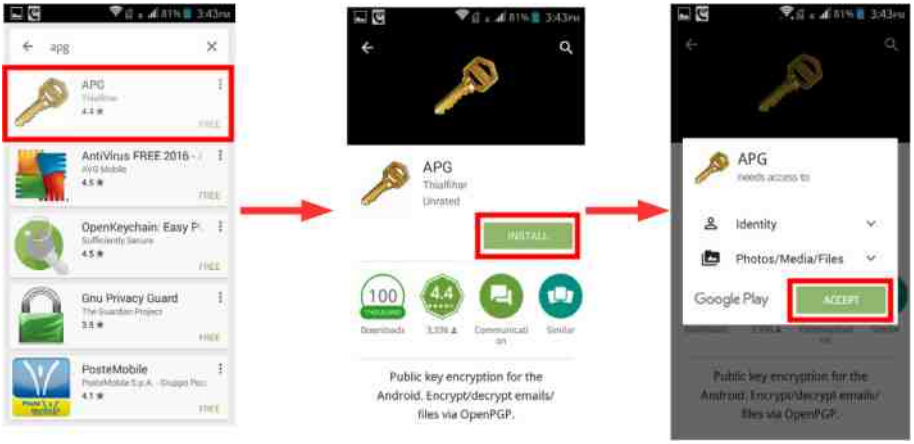
Аутор: Петар Симовић

Сви користимо имејл да комуницирамо, али како да са лакоћом размењујете шифровану електронску пошту на вашем андроид телефону користећи вашу постојећу имејл адресу? Да бисте могли и на Андроиду да примате и шаљете шифровану електронску пошту, потребан вам је програм за манипулацију ГПГ или ОпенПГП кључевима, као и имејл клијент. Најбоље је да оба програма буду отвореног кода (енг. *Open-Source*). За имејл клијента препоручујемо K-9Маил, а за ГПГ клијента АПГ или ОпенКиЧејн (енг. *OpenKeyChain*). K-9 мејл клијент ће радити са оба понуђена ГПГ клијента, а можете их преузети и са Гугл Плеј стора (енг. *Google Play Store*) и са Ф-Дроида (енг. *F-Droid*). Ми ћемо показати инсталацију, подешавања и размену шифрованих имејл порука користећи АПГ гпг клијента и K-9 имејл клијента.

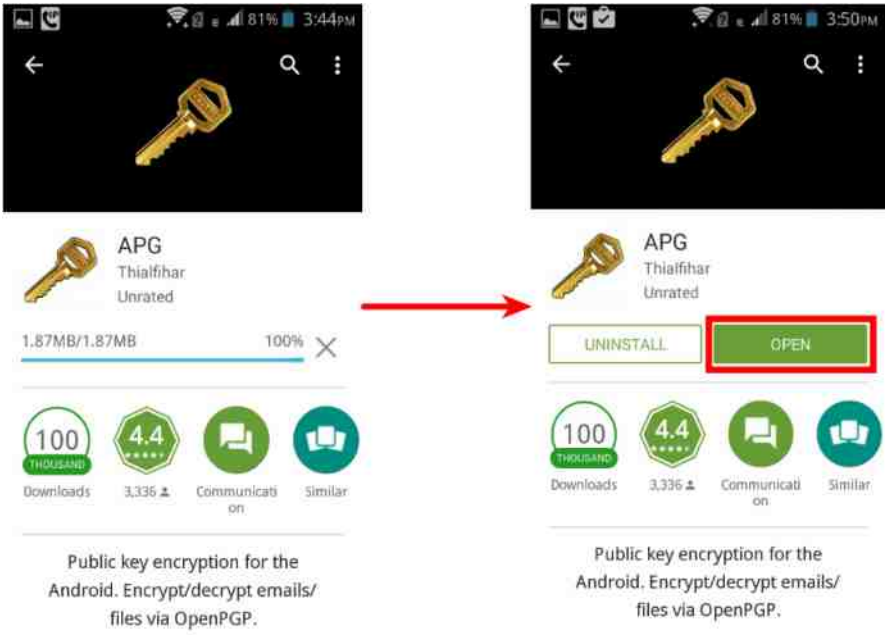
Инсталирање АПГ-а

Уколико имате инсталиран Ф-Дроид, онда препоручујемо да АПГ преузмете и инсталирате са Ф-Дроида (https://goo.gl/IMzcOE), или са Гугл Плеј стора (https://goo.gl/V38xkx).

Шифровање електронске поште на Андрооиду

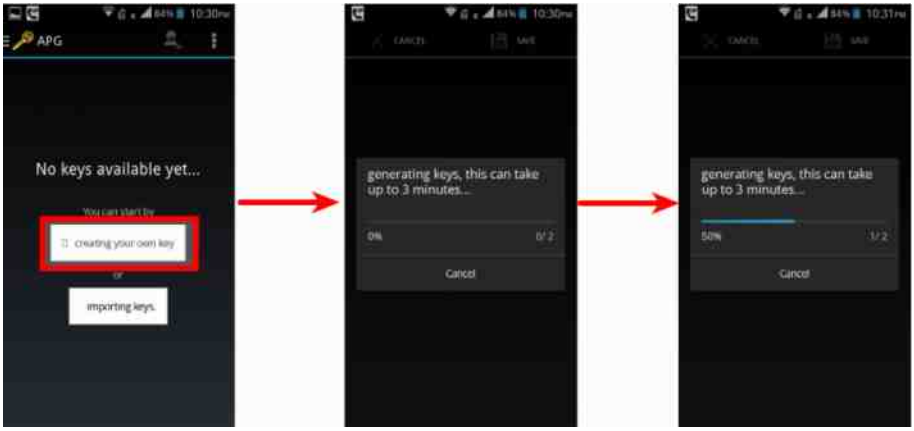


Када се инсталација заврши, покрените АПГ.

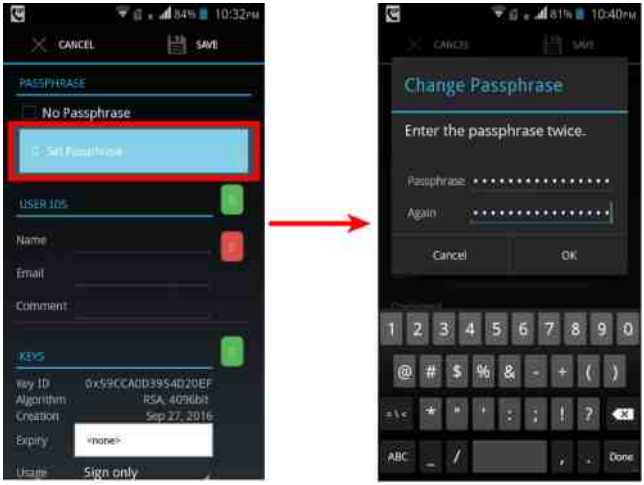


Подешавање АПГ-а

Када се инсталација заврши, покрените АПГ како бисте генерисали ваш нови ГПГ кључ за постојећи имејл.



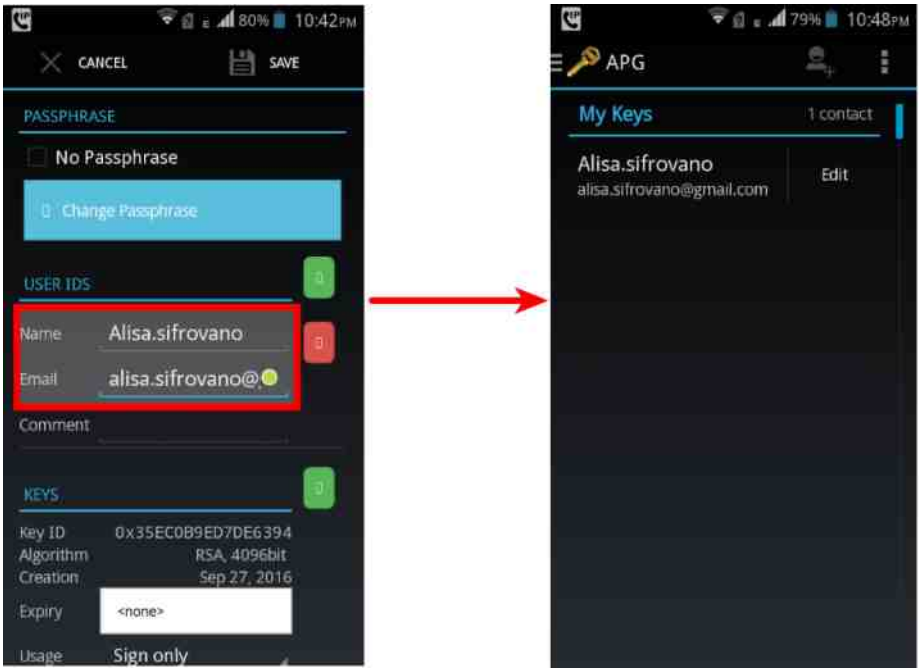
Одаберите опцију да креирате ваш нови кључ (енг. *„Create your own key”*). Уколико већ имате жељени ГПГ кључ за имејл адресу коју користите и на Андроид телефону, одаберите опцију за унос постојећег кључа (енг. *„import keys”*) и унесите јавни и тајни кључ са другог рачунара користећи УСБ кабл.



Шифровање електронске поште на Андрооиду

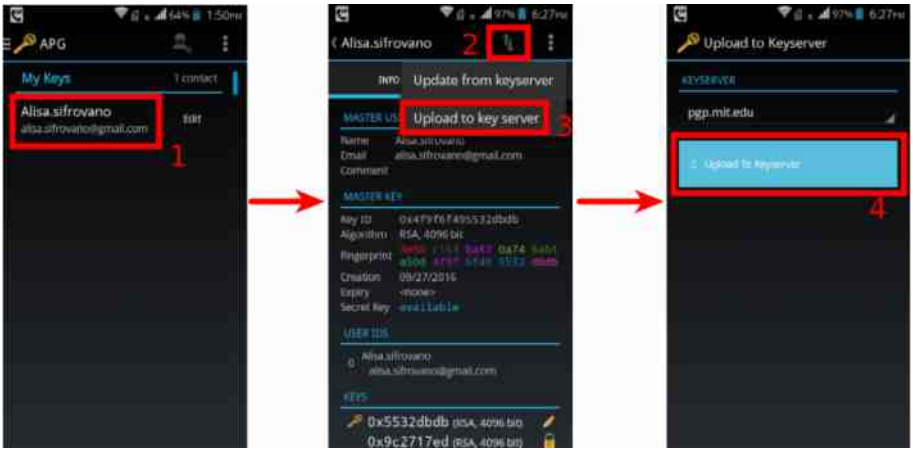
Када се кључ генерише, питаће вас да подесите ГПГ шифру за тај кључ. Овде обратите пажњу јер шифра мора да буде јака како би вас заштитила и у случају губитка кључева. Шифра за приступ вашем имејлу не би требало да буде иста нити да личи на шифру коју сте подесили за ваш ГПГ кључ. Саветујемо употребу малих и великих слова, бројева као и специјалних какрактера за шифру, као и да дужина шифре буде преко 12 карактера. Такође је могуће уместо једне дуге шифре користити фразу од неколико неповезаних случајних речи (као на пример: *„Correct Horse Battery staple"*).

Након постављања шифре за нови ГПГ кључ, додајте имејл адресу за коју сте генерисали кључ, име, као и опциони коментар ако желите. После овог корака смо завршили са подешавањима за АПГ, и прелазимо на инсталирање и подешавање имајл клијента који ће се ослањати на АПГ за операције шифровања, дешифровања, дигиталног потписивања и провере дигиталних потписа.



Објављивање вашег јавног кључа

Када креирате ГПГ кључ, желите да објавите ваш јавни кључ како би свако ко жели да вам пошаље шифровану поруку могао лако да сазна и набави ваш јавни кључ и њиме вам шифрује поруку.

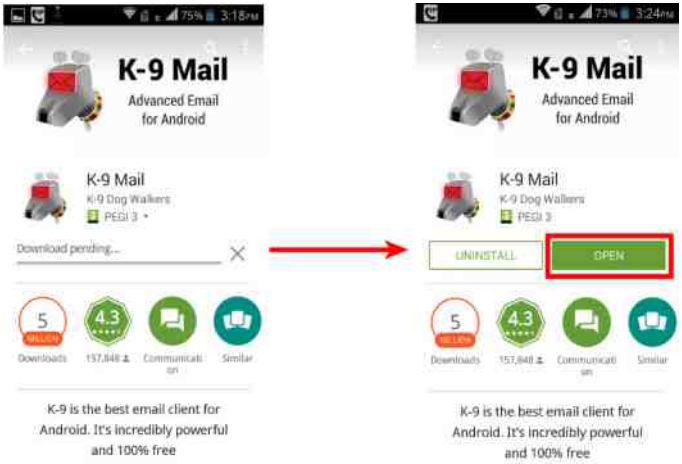


Пошаљите ваш јавни кључ из АПГ-а на сервер јавних кључева (енг. *key server*), у нашем случају сервер је https://pgp.mit.edu/ .

Инсталирање K-9 мејла

Како бисте лакше дешифровали примљене шифроване мејлове и слали шифроване мејлове другима, потребан вам је имејл клијент који препознаје да се ради о шифрованим порукама и у том случају се обраћа програму (АПГ-у) за подршку. Постоје и други клијенти поред K-9 мејла који подржавају шифровану електронску пошту ослањајући се на АПГ или Опенкичејн (енг. *OpenKeyChain*), али нису отвореног кода као АПГ. Да бисте инсталирали K-9 мејл, идите на Гугле Плеј стор (енг. *Google Play Store*, https://goo.gl/4tQTD), или на Ф-Дроид (https://goo.gl/yQejPh).

Када се инсталација заврши, покрените K-9 мејл.



Подешавање K-9 мејла

Када после инсталације покренете K-9 мејл, потребно је да подесите ваш имејл налог уношењем ваше имејл адресе (имејл адреса је она иста за коју сте креирали и ГПГ кључ, у нашем случају alisa.sifrovano@gmail.com) и шифре за приступ тој мејл адреси. Важно је разумети да постоје две шифре: једна за

приступ вашем мејлу у облику корисничког имена мејл адресе и шифре за то корисничко име, а друга шифра је за приступ вашем тајном ГПГ кључу кога сте малопре креирали помоћу АПГ програма. Шифра за ГПГ нема никакве везе са шифром за приступ вашем мејл налогу, и уколико изгубите ГПГ шифру и даље ћете моћи приступити мејл налогу и читати/писати нешифроване мејлове.

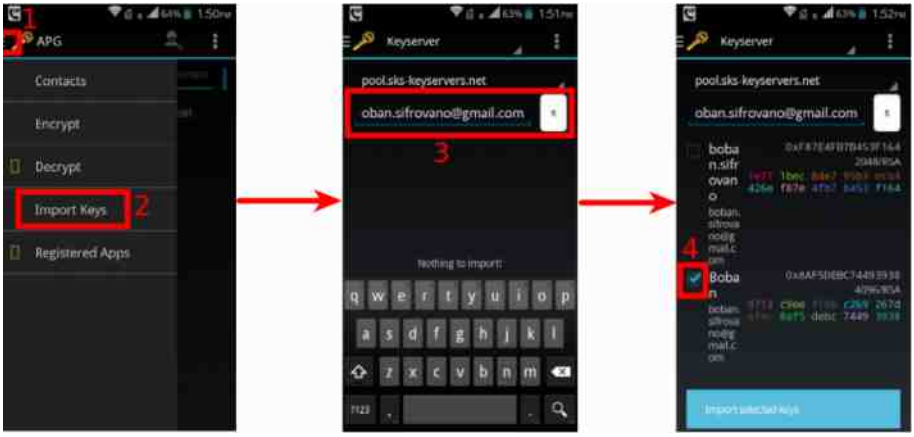
У K-9 мејлу унесите имејл адресу за коју сте правили ГПГ кључ и шифру за приступ том имејлу.

Размена шифрованих порука

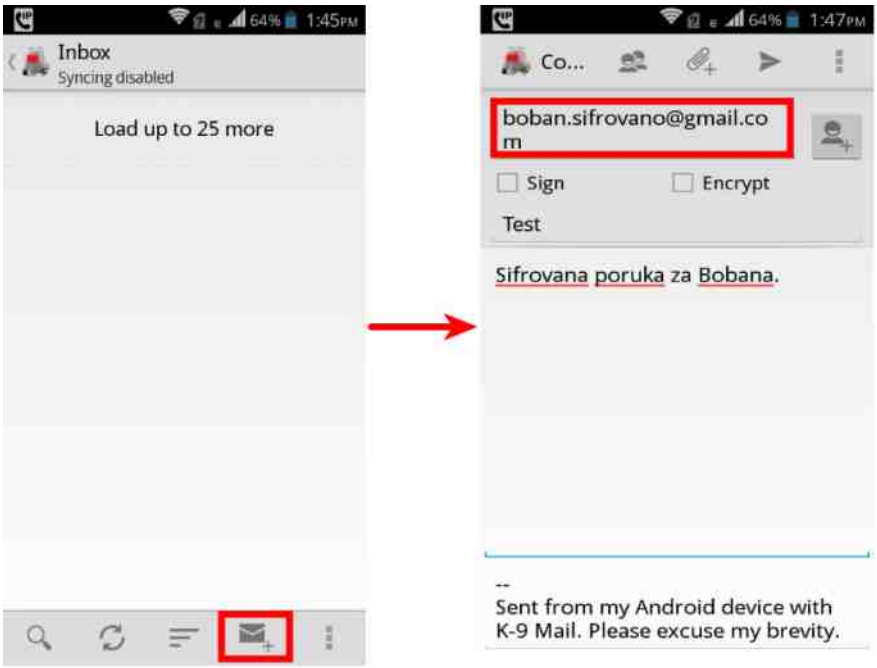
Набављање јавног кључа контакта

Да бисте послали шифровану поруку, потребан вам је јавни кључ контакта коме исту желите послати, исти јавни кључ вам је такође потребан да бисте проверили дигитални потпис примљене поруке истог контакта. Па хајде да преузмемо јавни кључ неког нашег контакта. Подразумева се да је и наш контакт такође креирао свој пар ГПГ кључева, као и да је послао јавни кључ на неки сервер јавних кључева. Напоменимо да није битно на који сервер јавних кључева сте ви послали ваш јавни кључ или ваш контакт јер се сви сервери јавних кључева међусобно синхронизују. Па тако, сваки кључ који се пошаље на неки сервер јавних кључева наћи ће се на свим осталима после отприлике десетак минута.

Шифровање електронске поште на Андрооиду

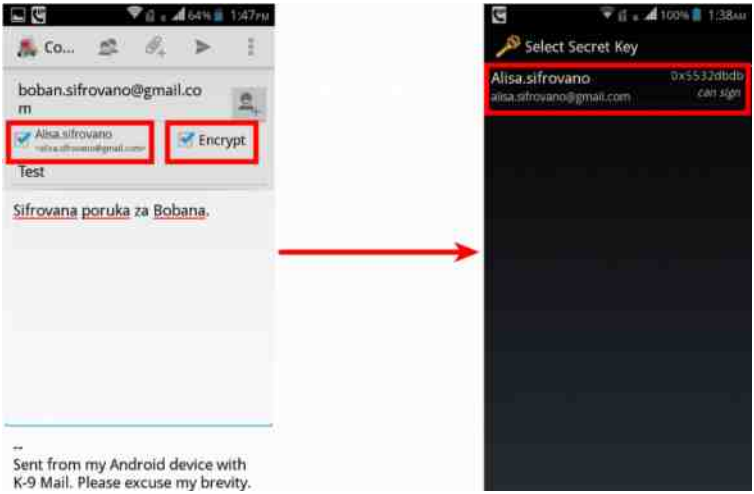


Слање шифрованих мејлова

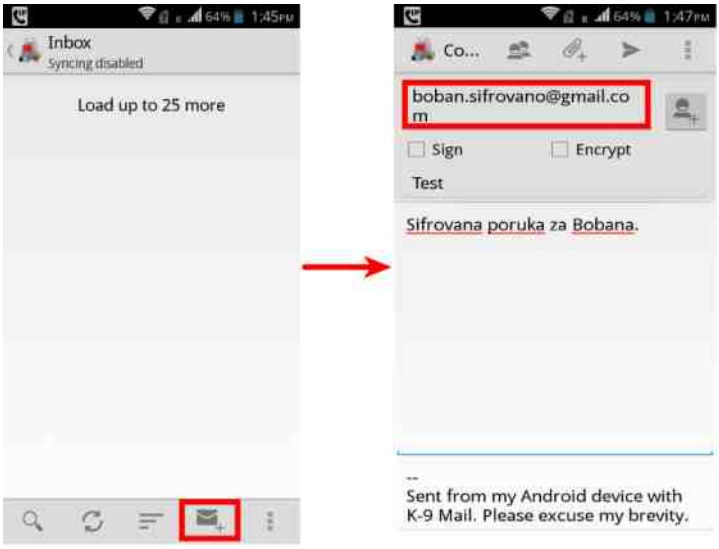


Мобилни кутак

Да бисте послали шифровану поруку, прво саставите исту и унесите имејл адресу примаоца чији сте јавни кључ претходно преузели.



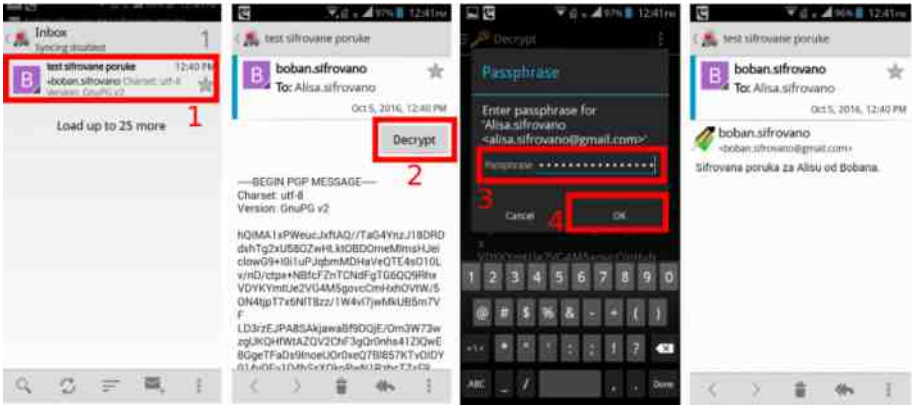
Када саставите поруку, одаберите опције за дигитално потписивање (енг. *Sign*) и шифровање (енг. *Encrypt*), и селектујете за потписивање ваш кључ.



И најзад, кликните на иконицу за слање поруке (папирни авиончић) и унесите вашу шифру за приступ вашем тајном ГПГ кључу како бисте приступили истом и дигитално потписали поруку поред шифровања.

Дешифровање примљених порука

Када вам неко пошаље шифровану поруку, потребно је да отворите K-9 мејл клијента, отворите примљену поруку, кликнете на дугме за дешифровање (енг. *Decrypt*) и унесете вашу ГПГ шифру. АПГ препознаје шифроване поруке унутар K-9 мејл клијента и понудиће да их дешифрује.

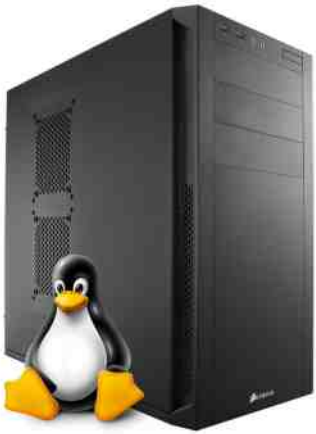


Када примите шифровану поруку у K-9 мејл клијенту, кликните на „Дешифруј" (енг. *Decrypt*) и унесите ГПГ шифру и то је то.

Хардвер

Састави сам свој Линукс кућни рачунар

Избор најбољих компоненти за 2016-ту годину



Аутор: Ненад Марјановић

Све је мање корисника који издвоје своје време да би се посветили одабиру компоненти за склапање кућног рачунара. Сем ако, наравно, изузмемо заљубљенике у видео игре. Први фактор је свакако недовољно познавање хардвера и техничких вештине које су ипак неопходне да се све састави, инсталира и изврши подешавање оперативног система. Такође, ту се понекад може испречити цена и фактор одлучности око изабира компоненти. Корисници се углавном одлучују за куповину преносних рачунара због њихове практичности и захтева коју доносе данашња комуникација и пословне обавезе.

За оне који ипак знају да квалитет долази са знањем, на основу искуства линукс корисника широм света наша редакција је направила селекцију компоненти које ћемо представити у овом чланку. За истраживње линукса довољно је купити и Расбери Пај (енг. *Raspberry Pi*), а за мало напредније кориснике конфигурације могу достићи и цену од пар хиљада евра.

Матична плоча

При избору матичне плоче треба размишљати о неколико важних детаља. Да подржава последњу генерацију процесора (*LGA1151*), да је модуларна (ово означава да временом можемо додати компоненте које нисмо могли укључити у конфигурацију на самом почетку) и, на крају, број конектора за спољашњи хардвер као што су ХДМИ/ВГА и УСБ последње генерације, 3.0. Што се тиче формата, данас се већина корисника одлучују за микро а-те-икс (енг. *micro ATX*). Разлог овоме је што у комбинацији са мањим кућиштима овако монтирани рачунари заузимају мало простора и могу стати на било који радни сто и уједно ниво буке је минималан. Гигабајт *GA-Z170M-D3H* поседује све ове предиспозиције и подржаће све модерне линукс системе. Када говоримо о подршци, у то спадају чипсетови (енг. *chipset*) који имају одличну подршку за бежични интернет и звук. Цена ове матичне плоче се креће око 120 евра.

Хардвер

ЦПУ (процесор)

Време је да се посветимо избору срца нашег будућег рачунара. Определили смо се да задовољимо свачије укусе, од корисника који искључиво користе рачунар за посету интернет портала, до оних који би желели да имају могућност за покретање виртуалних машина у циљу учења администрације система до особа заинтересованих за пентестинг и истраживање сигурности система и апликација. Наша одлука је Интел шесте генерација *i5* са четири језгра на радној фреквенцији од 3.4 гигахерца (турбо мод омогућава модификацију фреквенције до 3.9 гигахерца). Модел који смо тестирали је *i5-6600K*, чија је цена и даље висока (око 220 евра) али носи са собом све потребне особине процесора последње генерације. Овај процесор може служити и поносним гејмерима.

RAM (меморија)

До скоро смо сви причали о ДДР3 меморији, али као што то бива у информатици вођено Марфијевим законом, данас већ имамо ДДР4 меморију. За моћни процесор који смо изабрали и да бисмо искористили максимално његове могућности, изабрали смо два пута 8 гигабајта Корсар (енг. *Corsair*) ЛПХ ДДР4. Цена ове меморије је око 80 евра. Треба напоменути да горенаведена матична плоча може подржати до 32 гигабајта меморије.

ХДД, ССД или м.2

ХДД и ССД су и даље добра комбинација ако се одлучујемо око капацитета и брзине. Већина корисника данас користи ССД за инсталацију система, а ХДД за чување података, међутим овде говоримо о будућности и дугорочном решењу за наше потребе, тако да се треба одлучити за ССД. Тренутно модел који нуди најбоље решење по питању цене и перформанси је *Crucial MX* 250GB. Цена је око 100 евра.

Кућиште

Да бисмо негде удомили сав овај лепи материјал потребно нам је и кућиште. Избор је огроман, али на основу хардвера који смо већ предложили узећемо кућиште које подржава формат матичне плоче, као и алиментације. При избору кућишта би требало, поред горенаведених фактора, проверити мишљења других корисника да бисмо били сигурни да је ниво звучне изолације довољан да са нашим рачунаром можемо спавати у истој просторији. Наравно, ниво буке не зависи само од кућишта, али добро направљено кућиште може уклонити неминован звук вентилатора који су помало уморни од превелике употребе. На нашим просторима можемо пронаћи Кулер Мастер производе, али ту су и друге опције. Свако кућиште испод 40 евра је у већини случајева лошијег квалитета, тако да се треба добро распитати пре коначне одлуке.

Напајање

Увек на напајање треба гледати као на мотор који ће радити понекад и по неколико дана без престанка, а ако смо такви корисици, онда инвенстиција од 65 евра не би требало да нас блокира при избору, већ напротив, да нам обезбеди дуговечност осталих компоненти, својим стабилним радом. *Be Quiet! Pure Power L8 CF* је модел од 500W. Ако имате новца за модуларни модел, немојте се двоумити, зато што са тим типом напајања у кућишту можемо оставити само каблове који су нам потребни у датом тренутку, а остале можемо уклонити. Ово ипак остављамо у домен естетике која већини корисника није пресудна при одабиру.

Вентилатор процесора

Ово је део, поред матичне плоче, који ће појединцима одузети дане у потрази за најбољим решењем. Иако је све више рачунара са течним хлађењем, што пре само пар година није био случај због цене и техничке изводљивости, данас се модели вредни спомена крећу од 70 евра, али то ћемо оставити на избор искуснијим грађевинарима ПЦ небодера. На тесту смо скоро имали „мање" познату марку, која одлично ради свој посао, поготово ако не волите да чујете досадни шум који долази из кућишта.

При одабиру вентилатора треба водити рачуна да подржава тип процесора који користимо и наравно број децибела који смо спремни да поднесемо, или не. *Be Quiet! Pure Rock*, и ако сте у могућности да нађете верзију Блек, биће сасвим добро решење.

На крају остаје да заврнемо рукаве, дотакнемо неку металну површину и склопимо уређај који ће вредно радити у нашим домовима.

http://cryptoparty.rs