Дефинирање и воспоставување на рамка за лична безбедносна проценка на интернет корисник, Linux и Android системи

Проект по предметот Мрежна безбедност

Игнатиј Гичевски 131004

Вовед

Главниот проблем на сајбер безбедноста претставува справувањето со самата еволуирачка природа на областа. Сајбер просторот и целата негова подструктура се секојдневно изложени на познати, но и непознати напади. Апсолутна сајбер безбедност не постои, но со постојано надградување можеме значително да ја подобриме нашата безбедност како корисници во сајбер светот.

Во продолжение ќе се изврши еден осврт на алатките кои би можеле да го зајакнат интегритетот на Linux и Android системите и ќе бидат дадени неколку корисни совети при пристап на интернет за еден обичен корисник.

Алатките се поделени на 3 дела и тоа:

- Linux Security
- Internet Security
- Android Security

Во првиот дел се претставени неколку алатки кои можат дополнително да го осигурат веќе најбезбедниот оперативен систем, Linux. Програмите се тестирани и инсталирани на конкретна дистрибуција: Linux Mint 18.1 Serena.

Во делот за Internet Security најпрво се наведени неколку совети за зајакнување на прелистувачот, конкретно Google Chrome. Потоа се дадени неколку совети кои би можеле да ја зајакнат сигурноста на интернет корисникот без разлика на прелистувачот.

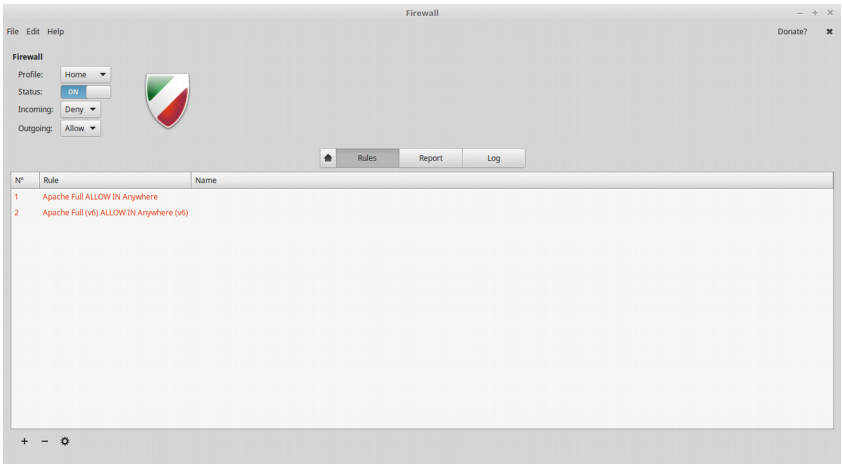
На крај, прикажани се и неколку first и third party алатки и совети за како да го заштитиме Android оперативниот систем. Алатките се тестирани и инсталирани на Android 5.0 Lollipop.

Linux Security

Конфигурација на Firewall

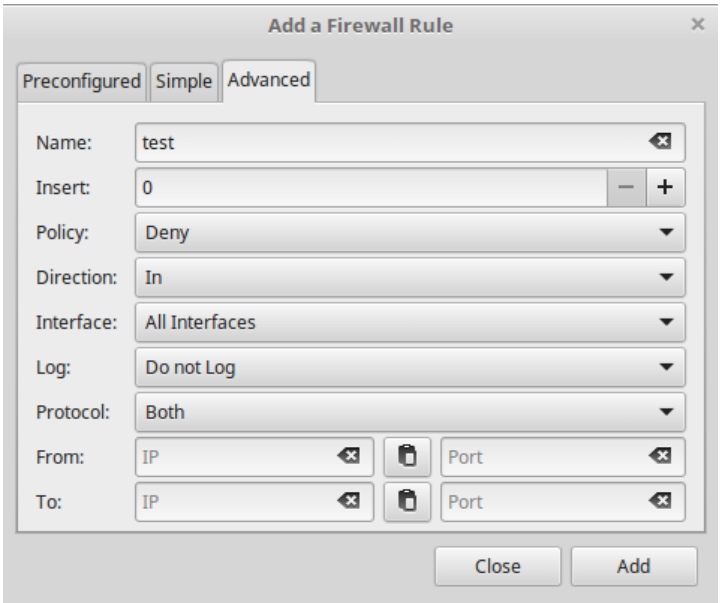
Linux Mint системите по инсталација доаѓаат со исклучен firewall и една од препорачаните работи по инсталација на Linux Mint е активација на firewall.

Тоа може многу лесно да се постигне со вградената програма ufw (Uncomplicated firewall). Ufw може да се конфигурира преку terminal или преку GUI. Програмата е едноставна и доста user-friendly и многу лесно може да се конфигурираат основни како и посложени правила за firewall.



Погоре на сликата дадени се основните препорачани правила за конфигурација на firewall на обичен интернет корисник (incoming: deny, outgoing: allow). Дефинирани се и две правила за Apache сервер.

Додавање на правила мануелно исто така е лесно. Конфигурацијата на правилата може да биде предодредена или внесена:



Бришење на cross-platform пакети

Mono, софтверската платформа што овозможува креирање и извршување на cross-platform апликации што се дел од .NET Foundation, доаѓа по default со оваа дистрибуција.

Со Mono, делумно се наоѓаме во инфицираниот екосистем на Windows. Mono е cross-platform што би значело дека може да биде основа за извршување на разни cross-platform malware и вируси и тоа претставува потенцијална опасност за самиот систем.

Sandbox: Firejail

Firejail е апликација која овозможува sandboxing на апликации. Го оневозможува пристапот на апликации до делови од системот каде и не треба да имаат пристап. На некој начин дава сигурност дека апликацијата која се извршува во sandbox-от и да е malicious, неможе да наштети на останатиот дел од системот.

Инсталација:

sudo apt-get install firejail

Извршување на firefox со firejail:

Password Manager: KeepassX

Бројот на апликации за десктоп кои се користат опаѓа, додека бројот на апликации кои се користат на интернет секојдневно се зголемува. Тој факт придонесува за тоа дека апликациите на web имаат свои форми за најавување со кои ги разликуваат корисниците.

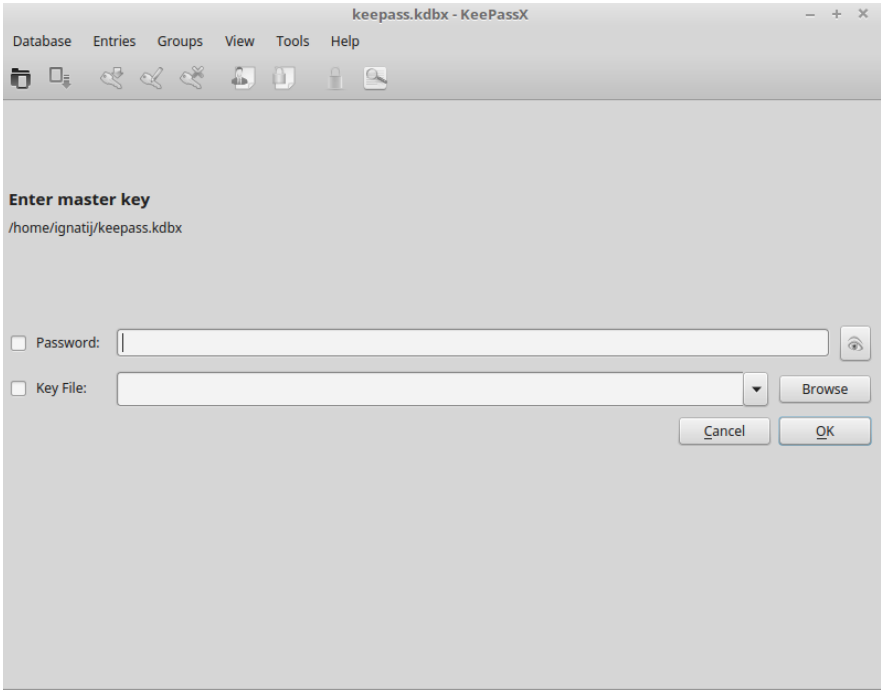
Најчесто начинот на најавување се состои од корисничко име и лозинка.

Од безбедносни причини, препорачано е еден корисник да нема иста лозинка за две различни апликации. Но, исто така знаеме дека тоа не е доволно бидејќи секоја лозинка треба да биде доволно силна (сложена) за да не биде пробиена.

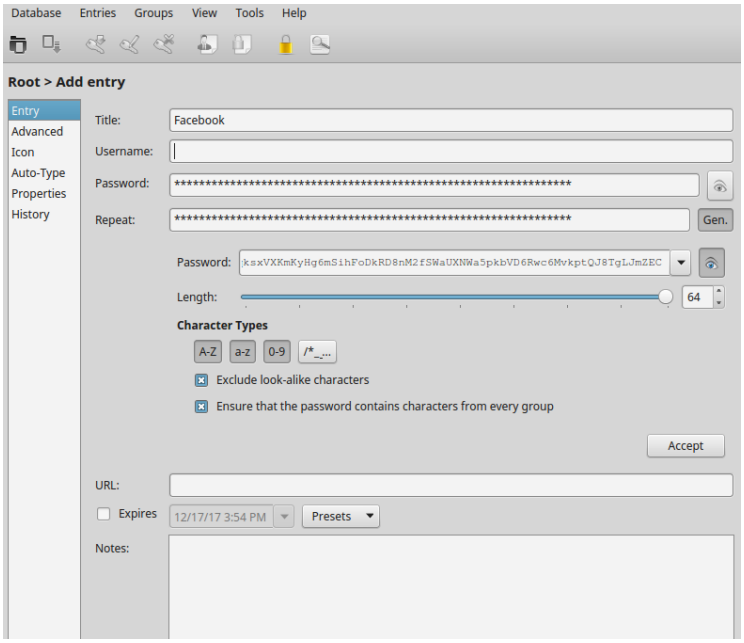
Ваквиот пристап од креирање на “јаки” и различни лозинки за секоја апликација посебно си има свои потешкотии.

Тука до израз доаѓа password manager. Keepass е програма за Windows системите која креира енкриптирана база локално каде што корисникот може да ги зачува своите лозинки. Верзијата на Keepass за Linux системите е KeepassX.

Потребно е еден master key за енкрипција на базата и потоа може да се додаваат лозинките како записи во таа база. Корисникот потребно е да го запамети само master клучот и сите лозинки што ги користи се веќе на дофат.



Исто така, при додавање на нов запис во базата, има и опција за рандом генерирање на лозинка до 64 карактери со големи/мали букви и специјални карактери.



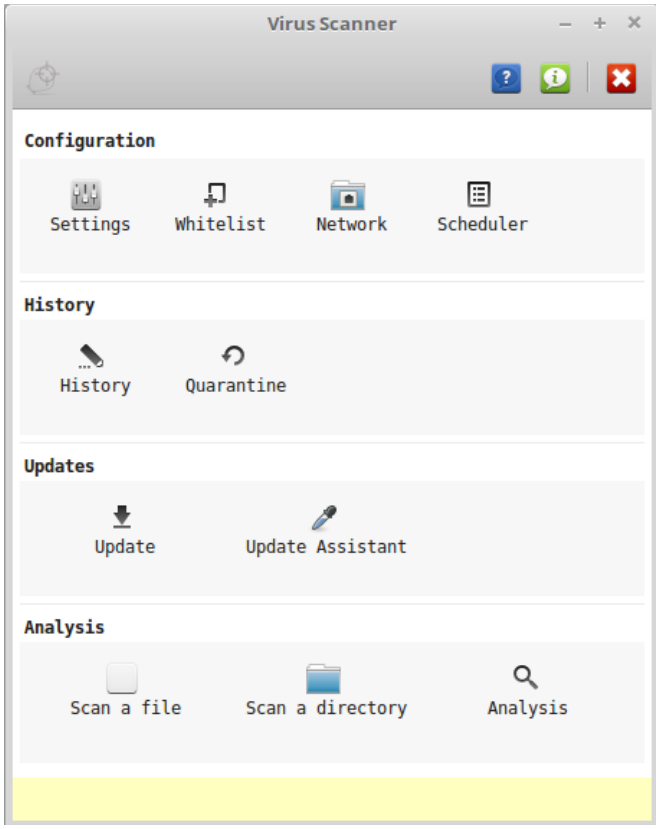
Malware Scanner: ClamAV

Генерално, на Linux системите не им се потребни анти-вирусни софтвери, но навремено скенирање на системот за потенцијални закани е секогаш добредојдено.

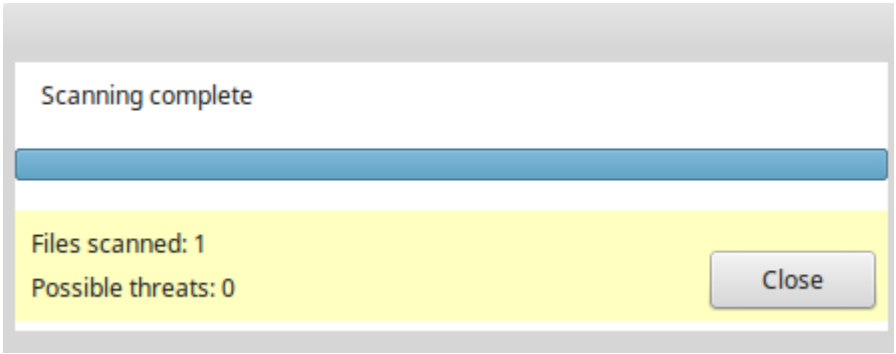
ClamAV е open source command-line алатка која овозможува скенирање на системот. Има и свое GUI верзија познато под името ClamTk.

Инсталација:

sudo apt-get install clamtk



Со ClamTk може да се скенира фајл, директориум или пак да се закажува дневно скенирање преку scheduler.



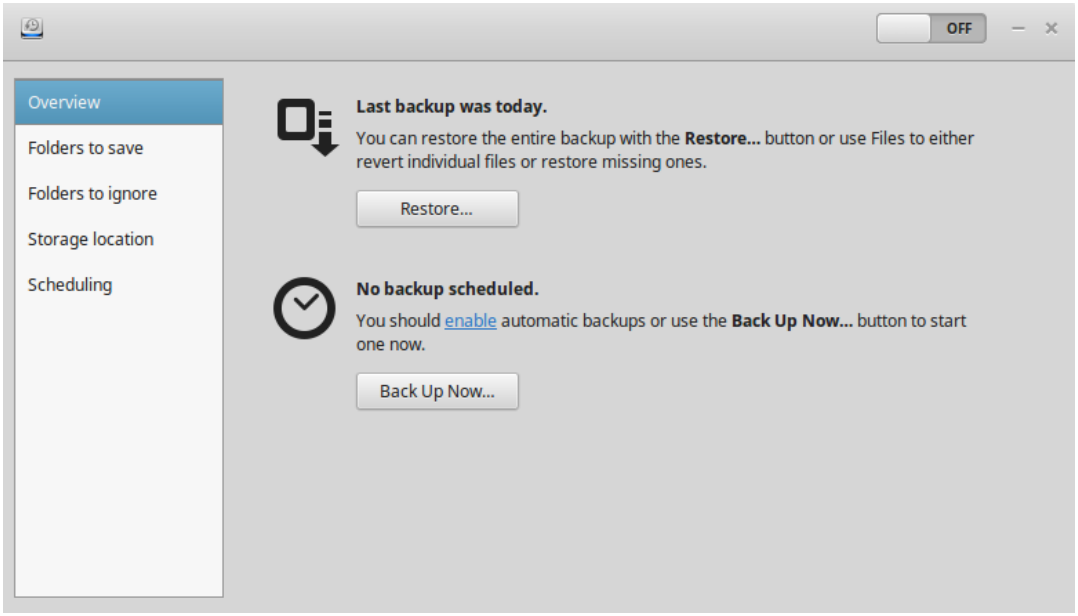
Backup software

Секој корисник треба понавремено да извршува backup на податоците. Linux системите можат да се пофалат со повеќе вакви алатки, во прилог прикажана е еден од поедноставните избори: Deja Dup.

Инсталација:

sudo apt-get install deja-dup

Алатката е едноставна и лесна за користење:



Корисникот може да избере кои фолдери сака да ги вклучи во backup-от и потоа да внеси и лозинка за да ги заштити податоците кои се вклучени во backup-от.

Алатката може да се извршува и од терминал:

deja-dup –backup

Internet security

Во втората половина на 2017 година, Kaspersky Lab објавиле извештај во кој тврдат дека околу 80 милиони уникатни URL-а се малициозни.

Безбедноста на прелистувачот е прва линија на безбедност против малициозни софтвери во веб апликациите. Во продолжение се неколку совети кои би ја подобриле безбедноста на прелистувачот.

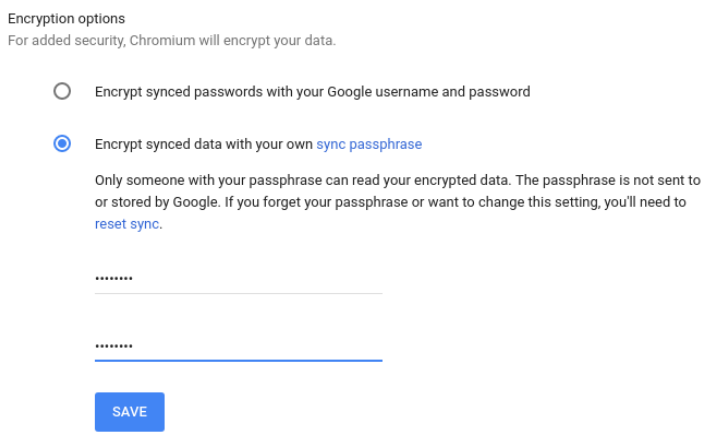
Деактивација на ActiveX – browser add-on што доаѓа преинсталиран со Internet Explorer или Microsoft Edge. Служи како middle man помеѓу PC и Java/Flash базирани интеракции на сајтовите. Претставува потенцијален безбедносен ризик бидејќи на малициозни сајтови им дава пристап на локален PC.

Деактивација на JavaScript – иако во денешно време скоро сите веб апликации побаруваат JavaScript поддршка за нивно извршување, сепак, доколку не сме сигурни во веродостојноста на веб апликацијата, не треба да дозволуваме JavaScript да се извршува. Бидејќи 93.6% од сите сајтови користат JavaScript, едно од главните оружја за можен напад е преку JavaScript.

Колачиња – деактивација на third party колачиња. Постојат 2 типа на колачиња: first party и third party колачиња. Првиот тип на колачиња се користат од истиот сајт каде што се наоѓа и корисникот, додека вториот тип на колачиња се користат од други места. Third party колачињата најчесто ги поставуваат advertisers и marketers кои се заинтересирани за online активностите на корисникот.

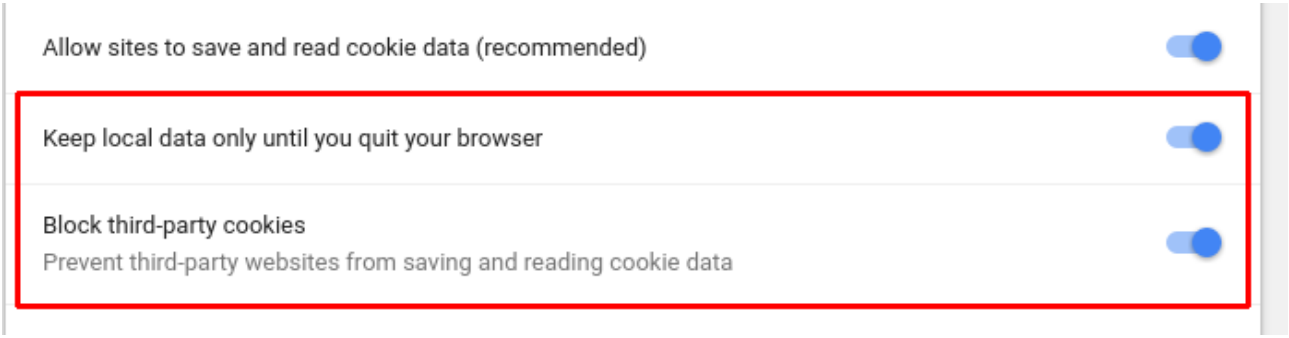
Securing Google Chrome

Во Settings, во делот Advanced sync settings, има можност да подесиме Encryption options. Default опција е Chrome да ги енкриптира податоците со корисничкото име и лозинка, но доколку некое лице ги дознае корисничкото име и лозинка, податоците како лозинки на корисникот, bookmarks и историјата на прелистувачот се веќе достапни.

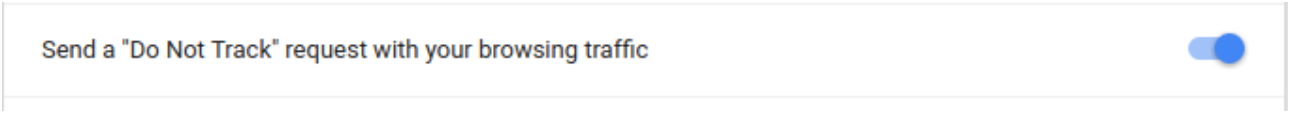


Во делот за колачиња, обележуваме да се чуваат локално податоците се до моментот кога прелистувачот се исклучува. Со тоа колачињата потоа се бришат.

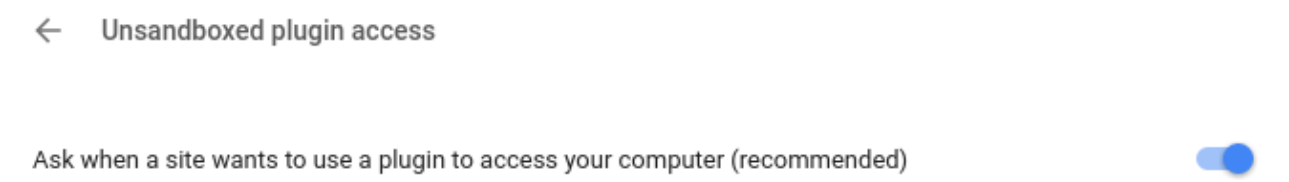
Ги блокираме third party колачињата.



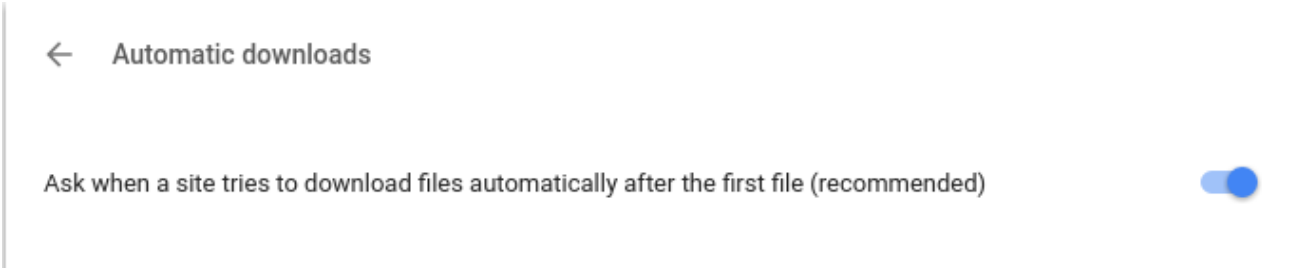
Во секцијата “Tracking”, ја одбираме опцијата “Do not track”, со која се праќа request за да не се врши влечење на кориснички податоци од страна на сајтот каде што моментално го посетува корисникот.



Во делот за Plugins, plugin-от треба најпрво да добие потврда од корисникот пред да започни со своето извршување:



И последно, за сите податоци кои се симнуваат од прелистувачот, корисникот треба најпрво да биде прашан пред да започне симнувањето.



AdBlock Plus – врши блокада на реклами, pop-ups, tracking, malware итн.

Disconnect – корисна екстензија која ги блокира third-party колачињата.
Исто така, врши блокирање и на секаков обид од страна на било која социјална мрежа за влечење на кориснички податоци како историја на прелистувач и приватни податоци.

Ghostery – алатка која блокира trackers и ја подобрува работата на прелистувачот.

Во продолжение се неколку корисни совети за зачувување на интегритетот на интернет корисникот, независно од прелистувачот.

1. **Уникатни лозинки за секој нова корисничка сметка** -тука до израз доаѓаат password managers.

2. **VPN** - при секоја конекција кон интернет доколку се користи несигурна (јавна) безжична врска, препорачливо е конекцијата да се врши преку VPN, со што се овозможува таа врска да биде енкриптирана и тешка за пробивање. Но, најдобрите VPN сервиси како што се NordVPN (2.75$), IPVanish (7.50$), PureVPN (47.76$ y), KeepSolid(18$) доаѓаат со месечна/годишна доплата.

3. **Дво-факторна автентикација** - додава уште еден слој на безбедност што треба да се помине покрај класичниот начин што се состои од корисничко име и лозинка. Најчесто, во сајбер светот, вториот фактор на автентикацијата се одвива според правилото “something you own” и најчесто претставува внесување на некаков код кој е претходно испратен на телефонот.

4. **Користење на различни email адреси за различни кориснички сметки**

5. **Редовно чистење на кешот на прелистувачот**

6. **Исклучување на “Save password” на прелистувачот** - најбезбедно е прелистувачот да не зачувува никакви лозинки на корисникот, туку да се користи password manager локално за справување со лозинки.

7. **Бришење на кориснички сметки кои повеќе не се користат**

8. **Подобра заштита на “Password Reset” услугата** - неколку сајтови веќе вклучуваат опција како: “Require personal information to reset my password”, со која се побарува од корисникот да внесе и дополнителна информација за да изврши ресетирање на лозинката.

9. **Проверка на “Account activity”** - Facebook, Google веќе имаат вградено опција со која може корисникот да ја провери својата најскора активност.

11. **Специфицирање на trusted contacts** - ова е опција што ја нуди Facebook, имено доколку некако дојде до компромитирање на корисникот, тој може да си ја поврати корисничката смета со помош на кодови пратени од Facebook до претходно наведени 3-5 пријатели.

12. **Промена на лозинка редовно**

13. **Во тек со најновите трендови и случувања во област на сајбер безбедноста**

14. **Безбедно сурфање -** претпазливо да не се кликнува на линкови/реклами/pop-ups кои можат да бидат линкови до phishing сајтови, или линкови со кои би овозможиле симнување на малициозен софтвер. Исто така, да не се врши споделување на пре-сензитивни и приватни информации по социјалните мрежи.

Android Security

Во продолжение се опишани неколку корисни апликации кои придонесуваат за подобрување на безбедноста на Android оперативниот систем.

Некои од апликациите се од самиот Android оперативен систем, додека некои се third-party.

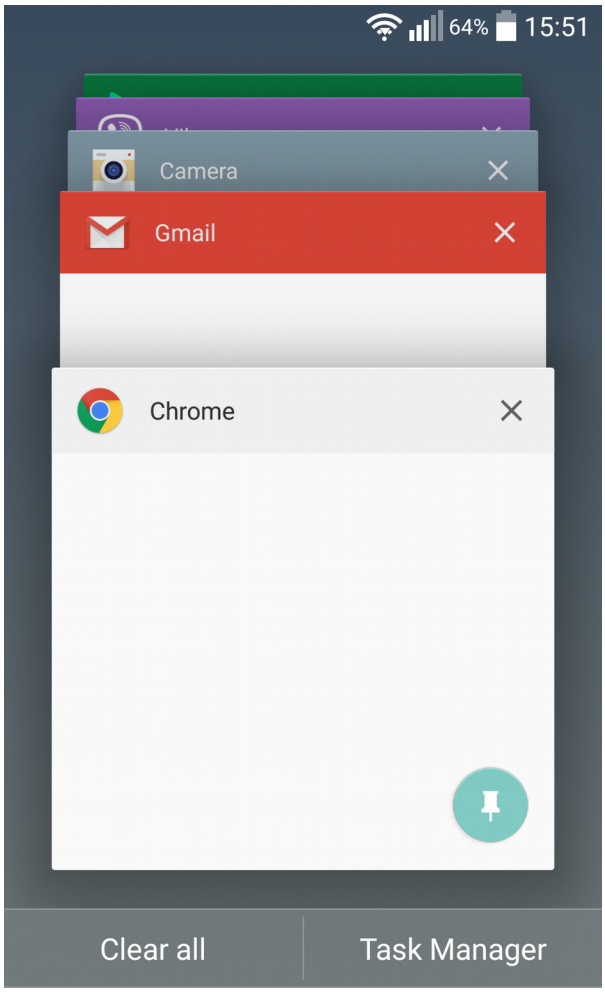
Screen pinning

Вграден feature од страна на Android правејќи го своето деби од верзија 5.0 Lollipop.

Овај feature овозможува заклучувањето на екранот на конкретна апликација, па за повторно отклучување на екранот потребно е да се внеси лозинка или некаков pattern.

Со овај feature личноста што го поседува моментално телефонот е оневозможена од извршување на други активности освен апликацијата која што е моментално заклучена.

Со кликање на pin-от до апликацијата се овозможува заклучување на екранот.



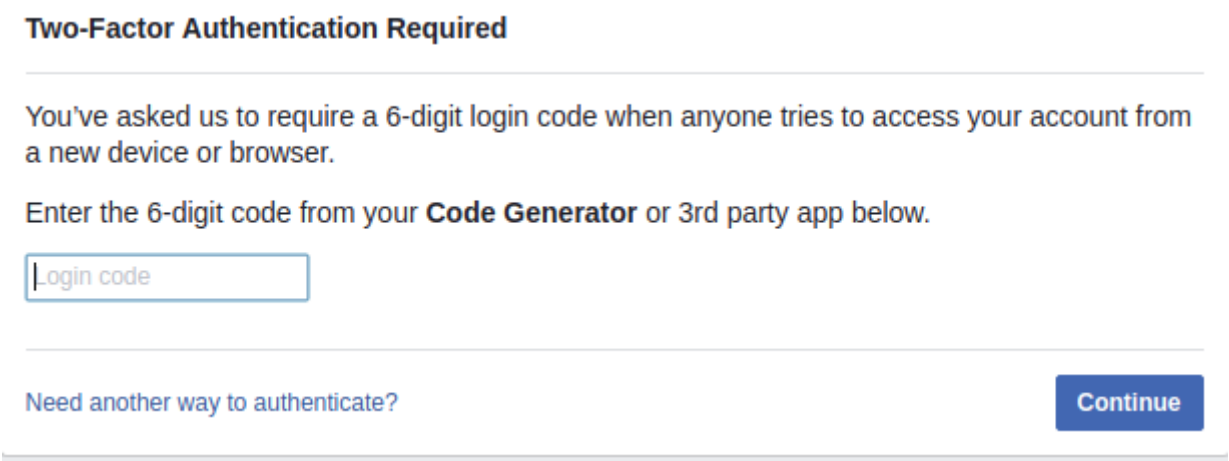
Дво-факторна автентикација

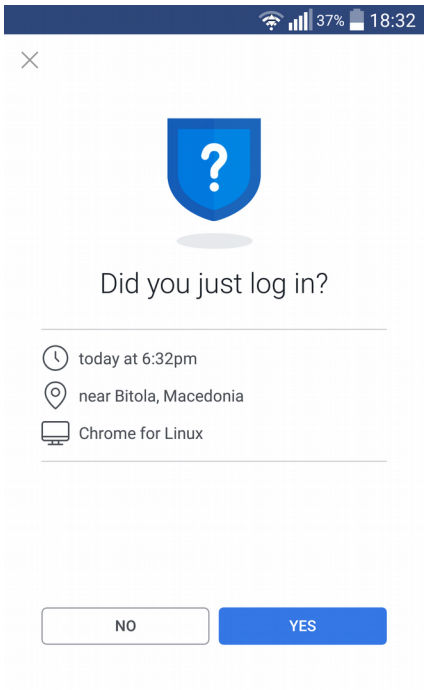
Доста популарен избор за извршување на дво-факторната автентикација е апликацијата Authy.

Апликацијата е доста позната по тоа колку лесно корисникот може да воспостави ваков начин на автентикација. Веб апликациите во Security Settings имаат опција да дозволат да се извршува дво-факторна автентикација преку third-party апликации.

Тие даваат QR код кој што само се скенира со помош на Authy и веќе дво-факторната автентикација е поставена. Потоа, при обид за логирање преку непознати уреди, се испраќа барање до апликацијата и корисникот одлучува дали ќе се изврши или не автентикацијата.

Се што треба да направи корисникот е да избере “Yes”/“No”, потоа Authy автоматски се поврзува со логирањето и прави редиректирање во зависност од изборот на корисникот, додека 6-цифрениот код корисникот нема потреба воопшто да го внесува.





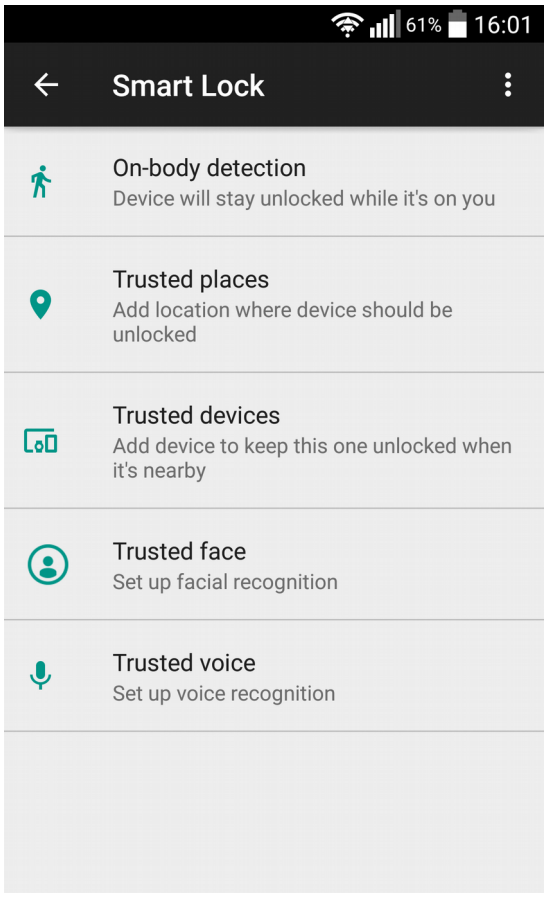
Android Smart Lock

Pattern, пин, лозинка се едни од неколкуте начини за отклучување на телефонскиот уред. Но, бидејќи за секое користење на телефонот треба одново да се поминува низ еден од претходно споменати методи на автентикација, процесот знае да стате доста заморлив.

Заради тоа, доста корисници ги скокаат сите механизми за автентикација и со тоа нивото на безбедност на нивниот уред е намалено до минумум.

Android Smart Lock е feature кој го носи најдоброто од двата света. Односно, Smart Lock нуди неколку опции Android да не го заклучува мобилниот уред кога:

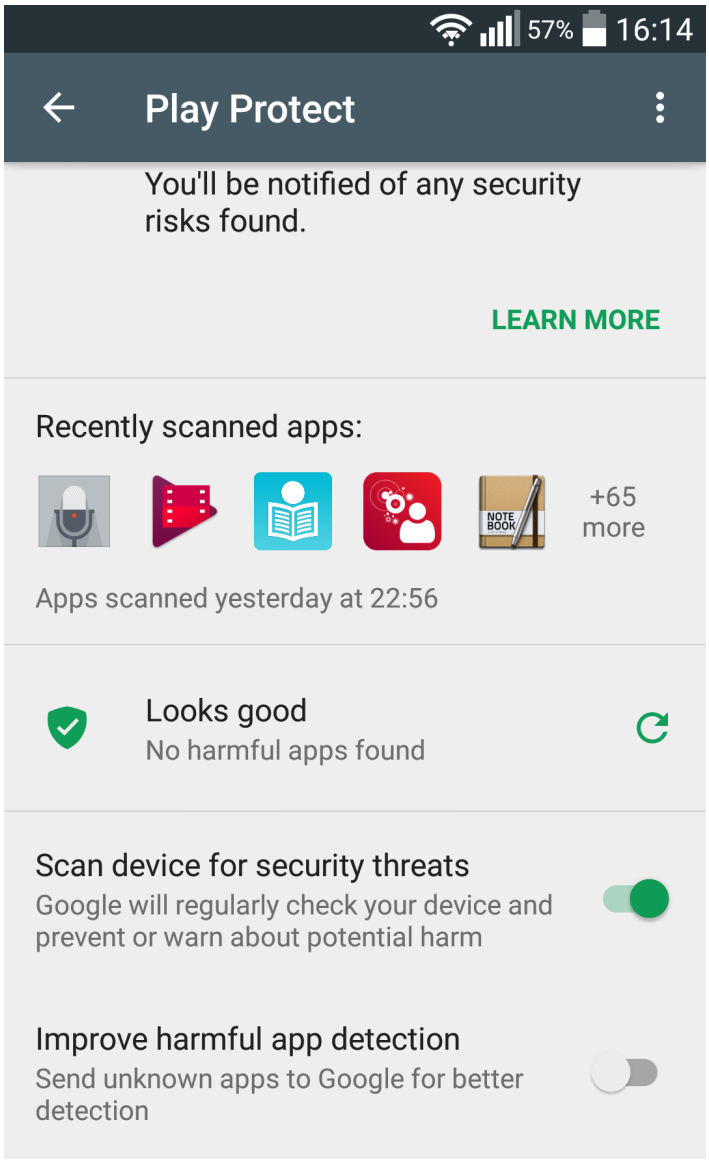
- мобилниот уред е во рацете на корисникот
- мобилниот уред се наоѓа на некоја локација која што е наведена како trusted
- мобилниот уред се наоѓа во близина на некој друг уред кој што е наведен како trusted
- facial recognition
- voice recognition



Скенирање на апликации

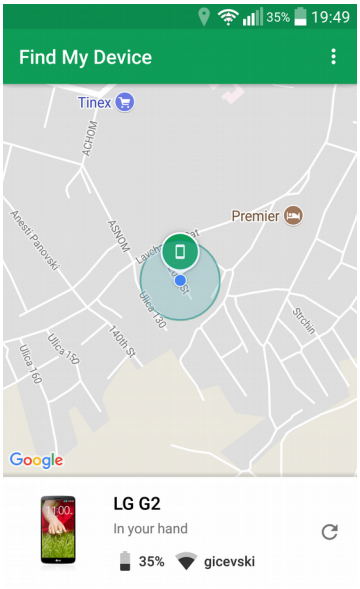
Започнувајќи од 2012, Android има вградено feature за скенирање на системот за малициозни знаци. Овај feature не само што прави скенирање на апликации при нивната инсталација, туку прави и повремено комплетно скенирање на целиот уред.

Доколку не е активиран по default, овај feature може да се активира во Settings/Google Settings на уредот.

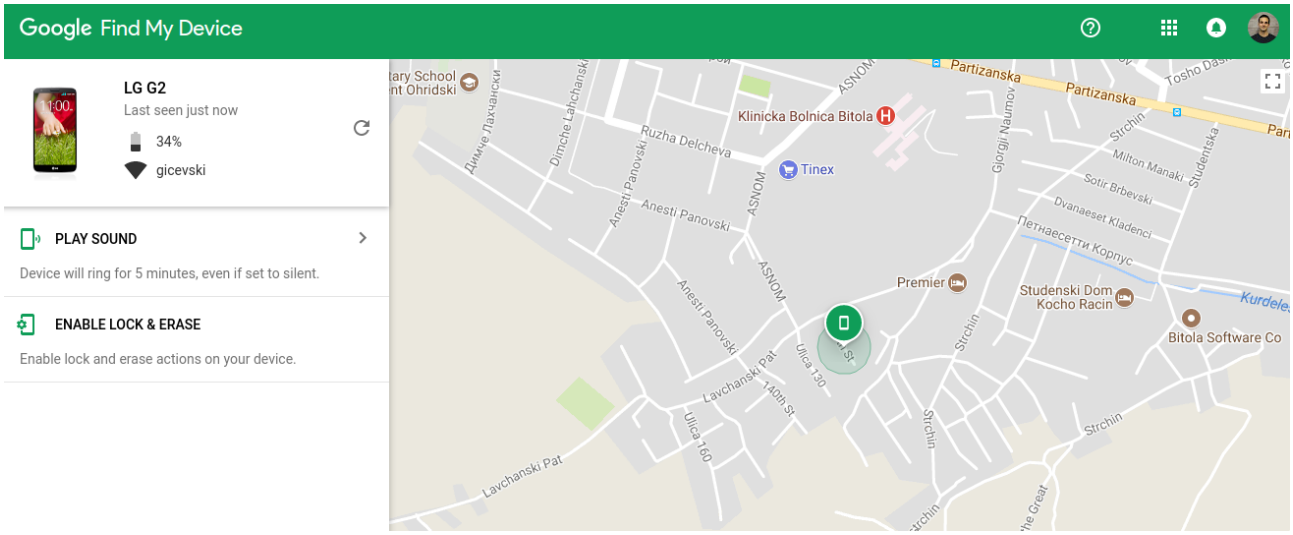


Find device

Апликација која што овозможува корисникот да си го пронајде мобилниот уред преку некој друг уред.



Веб верзијата на апликацијата овозможува и дополнителни опции како што се 5 минутно звонење или заклучување на мобилниот уред.



Android VPN

Иако не доаѓа во free верзија, доколку корисникот често користи јавни Wi-Fi, тогаш вреди да се размисли за неколку долари месечно за да се осигура безбедноста на комуникацијата.

Препорачана апликација за VPN е SurfEasy, изработена од компанијата која што го има изработено прелистувачот Opera. Апликацијата е претпознатлива по тоа што е лесна и едноставна за конфигурација и користење. Доаѓа и со разумна цена од 3 долари месечно.

Password managers

Решение на проблемот со менаџирање на лозинките постои и на Android уредите, апликацијата LastPass. LastPass овозможува и зачувување на информации на лични документи како ID, пасош...

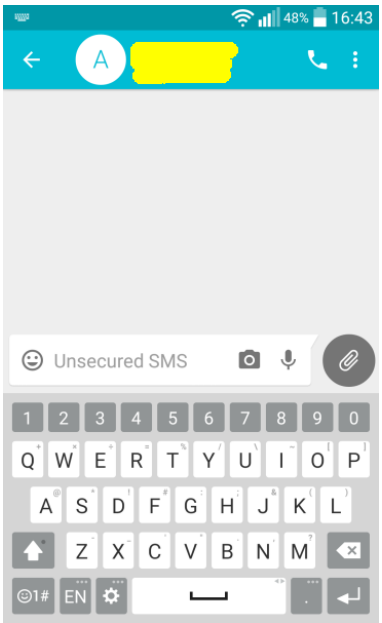
Информациите што се зачувани во LastPass се енкриптирани со AES-256.

Апликацијата побарува од корисникот да запамети само една лозинка (master лозинка) за декриптирање на зачуваните информации. Овозможува генерирање на “јаки” лозинки и автоматско пополнување на полето при најава на некоја апликација чии што credentials се зачувани во LastPass.

LastPass доаѓа со доплата од 12 долари на годишно ниво.

Signal

Signal е free и open-source апликација која овозможува end-to-end енкрипција на комуникацијата, без зачувување на информации на серверска страна.



Изработена од Open Whisper Systems, единствениот приватен messenger кој користи open-source peer-reviewed криптографски протоколи за зачувување на интегритетот на пораките.

Апликацијата функционира и со стандардни SMS пораки, дури и ако клиентот што ја прима пораката не ја користи апликацијата, Signal додава уште еден слој на безбедност врз пораката.

Edward Snowden редовно изјавува на Twitter за апликацијата.

Haven: Keep Watch

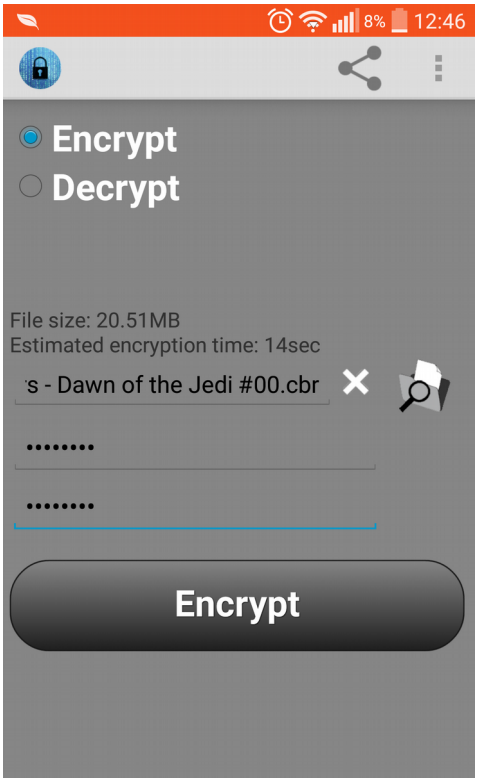
Уште една апликација позади која стои името на Snowden, Haven е se уште во бета верзија и служи за претворање на телефонскиот уред во уред за мониторинг и систем за надгледување. Апликацијата е производ на колаборацијата помеѓу The Guardian Project и Freedom Of The Press Foundation.

Апликацијата ќе ги известува корисниците кога ќе забележат движење во просторија во која се наоѓа лаптоп или друга важна опрема, ќе снима звук, а може дури и да преведе влез од акцелеметар на телефонот со цел да одреди дали телефонот е поместуван.

Crypt4All Lite

Crypt4All Lite е free апликација која овозможува енкрипција и декрипција на податоци од телефонскиот уред.

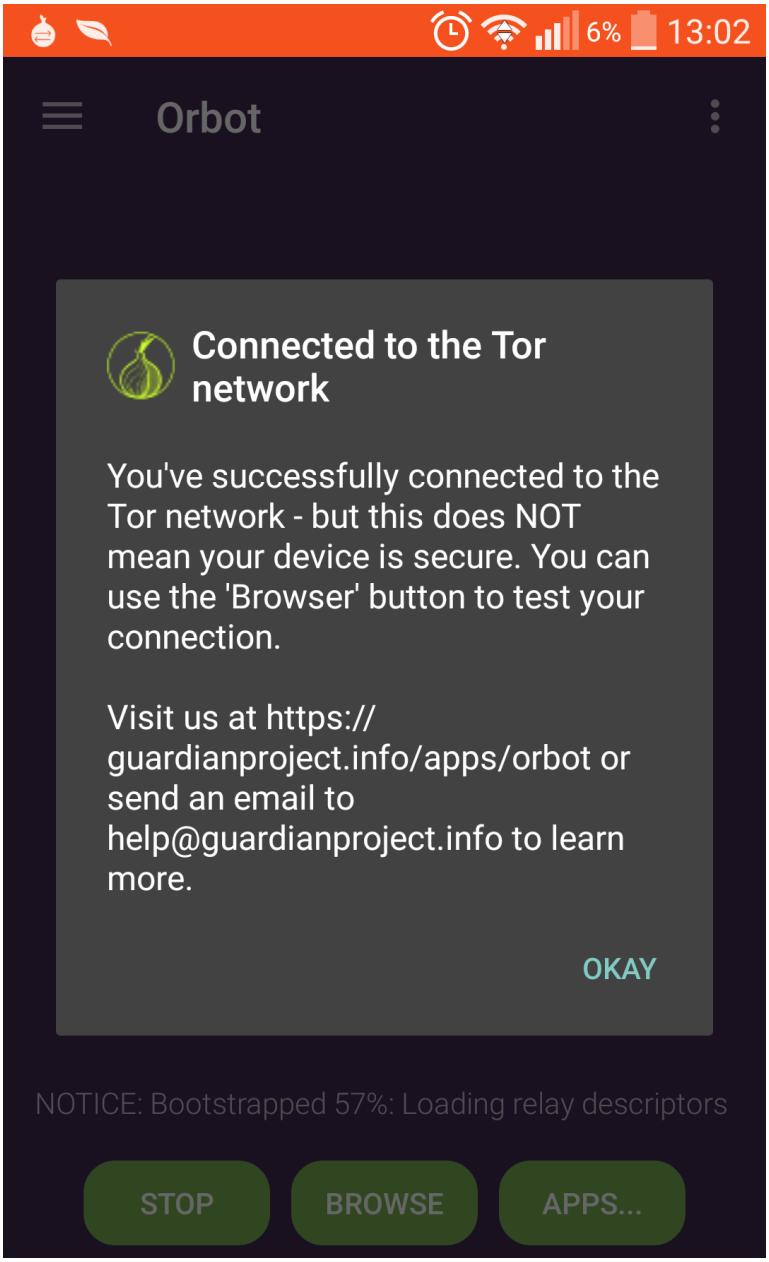
Енкриптирањето и декриптирањето се врши со AES-256. Една примена на апликацијата е при префрлување на сензитивни податоци од телефонот на cloud системи, ги енркиптираме податоците и во мобилниот уред остануваат како енкриптирани податоци.



Orbot и Orfox

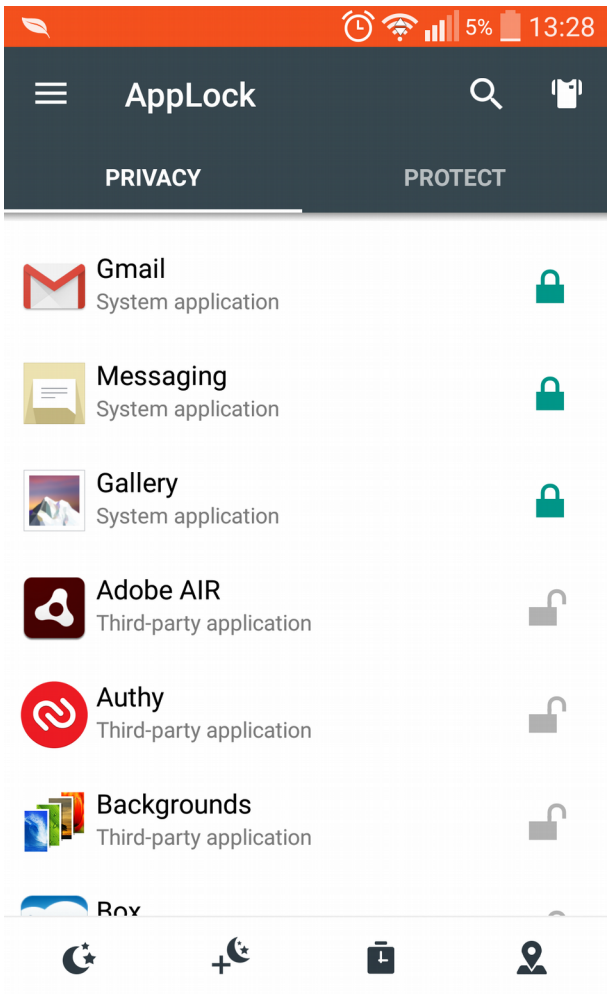
Orbot е бесплатна proxy апликација која го користи Tor за криење и енкрипција на интернет сообраќајот.
Orfox е мобилен прелистувач чија што основа е истиот код како што е Tor Browser, само со посебна модификација да работи врз Android платформата.

Orbot и Orfox се изградени од тимот The Tor Project.



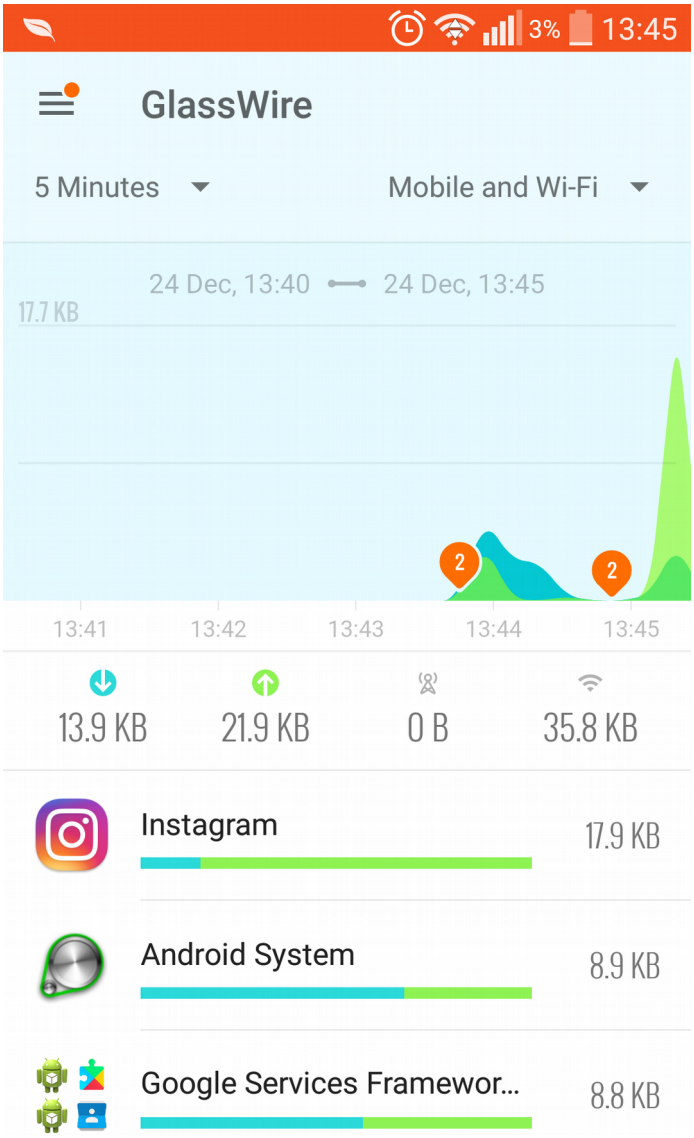
AppLock

AppLock е апликација која овозможува заклучување на апликациите. При пристап до некоја заклучена апликација, потребно е да се внеси лозинка или да се нацрта pattern за нивно отклучување.



Glasswire

Glasswire овозможува детален преглед како апликациите користат интернет преку live graph. Исто така, апликацијата праќа алерти во случај ако некоја нова апликација почнува да користи интернет конекција. Одличен начин за да се види дали има некоја чудна активност што се извршува во позадина.



Референци

http://www.makeuseof.com/tag/firejail-simple-way-improve-security-linux/

https://sites.google.com/site/easylinuxtipsproject/mint-cinnamon-first#TOC-Turn-on-the-firewall

http://www.makeuseof.com/tag/keepassx-secure-password-management-linux-os/

http://www.tuxgarage.com/2011/06/deja-dup-ubuntu-installation-and-usage.html

http://www.makeuseof.com/tag/security-tools-linux/

https://securelist.com/it-threat-evolution-q1-2017-statistics/78475/

https://heimdalsecurity.com/blog/javascript-malware-explained/

https://heimdalsecurity.com/blog/ultimate-guide-secure-online-browsing/

https://adblockplus.org/

https://www.pcmag.com/article2/0,2817,2403388,00.asp

https://www.pcmag.com/article2/0,2817,2478462,00.asp

http://fieldguide.gizmodo.com/18-ways-to-make-your-online-accounts-more-secure-1793250264

https://www.computerworld.com/article/3029725/android/7-android-tools-that-can-help-your-personal-security.html

https://thehackernews.com/2015/04/android-privacy-security-apps.html

https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms&hl=en

https://www.androidauthority.com/best-security-apps-android-687799/

https://twitter.com/snowden/status/778592275144314884

http://denar.mk/165441/tehnologija/snouden-napravi-aplikacija-koja-stiti-od-natprapnici