ЯК ВЕСЬЦІ БЛОГ **АНАНІМНА**

Этан Цукерман (Ethan Zuckerman)

Гэты кароткі тэхнічны дапаможнік па ананімнаму вядзеньню блога – спроба падыйсьці да праблемы з боку чалавека, які паведамляе пра злоўжываньне становішчам членам ўраду, дзейнасьць якога далёка не празрыстая.

Гэты дапаможнік не для кібэрпанкаў, але для людзей з разьвіцьцёвых краін, якія ня ўпэўненыя ў сваёй бясьпецы і хочуць даведацца, як на практыцы забясьпечыць сваю ананімнасьць. Дапаможнік "Як бясьпечна весьці блог" ("How to blog safely"), падрыхтаваны Фондам "Электронная мяжа" ("The Electronic Frontier Foundation") (http://www.eff.org/Privacy/Anonimity/blog-anonymously.php), таксама прапануе шэраг карысных парадаў на гэтую тэму.

ЗЬМЕСТ

Знаёмства з Сарай
Крок 1 Псэўданімы
Крок 2 Агульнадаступныя кампутары
Крок 3 Ананімныя проксі-сэрвэры
Крок 4 Гэтым разам усё надзейна!
Крок 5 Цыбулінная маршрутызацыя (onion routing) праз Tor
Крок 6 MixMaster, Invisiblog і GPG
Якая аптымальная ступень ананімнасьці? Дзе трэба спыніцца?

ЗНАЁМСТВА З САРАЙ

Сара працуе бухгалтаркай ува ўрадавай установе. Яна даведваецца, што яе начальнік, намесьнік міністра, крадзе вялікія сумы грошай у дзяржавы. Яна хоча, каб сьвет даведаўся пра гэтае злачынства, але баіцца згубіць працу. Калі яна паведаміць пра злачынства міністру (калі толькі ў яе атрымаецца да яго прабіцца!), яе могуць звольніць. Яна тэлефануе рэпартэру мясцовай газэты, але той кажа, што для артыкула трэба нашмат болей інфармацыі, а таксама дакумэнты, якія б пацьвярджалі яе падазрэньні.

Такім чынам, Сара вырашае распачаць уэблог, каб расказаць сьвету пра тое, што ёй вядома пра цёмныя справы ў Міністэрстве. Каб абараніць сябе, Сары трэба быць упэўненай, што ніхто ня зможа даведацца, хто яна, з яе нататкаў у блогу. Ёй трэба весьці блог ананімна.

Калі яна распачне ананімны блог, яе можна вылічыць двумя шляхамі. Першы: гэта можна зразумець са зьмесьціва. Напрыклад, калі яна піша: "Я працую памочніцай галоўнага бухгалтара ў апараце міністра вугальнай прамысловасьці", даволі хутка можна даведацца яе імя. Другі: на падставе інфармацыі, атрыманай праз уэб-браўзэры і паштовыя праграмы. Кожны кампутар, падключаны да інтэрнэту, мае свой асобны ці сумесны IP-адрас. Гэта набор з чатырох нумароў ад 0 да 255, аддзеленых кропкамі, напрыклад: 213.24.124.38. Калі Сара разьмяшчае свае нататкі ў інтэрнэце з дапамогай уэб-браўзэра з працоўнага кампутара, то IP адрас уключаецца ў яе паведамленьне.

Не прыклаўшы вялікіх намаганьняў, кампутаршчыкі ў міністэрстве высьветляць асобу Сары па гэтым IP адрасе.
Сара вырашае зьвязацца з правайдэрам інтэрнэт-паслуг (ISP) з дапамогай мадэма з дамашняга кампутара. Але кожны правайдэр фіксуе, які IP адрас меў канкрэтны

тэлефонны нумар у дадзены час. У адных краінах міністру будзе патрэбны сьпецыяльны дазвол на атрыманьне такой інфармацыі, у іншых (асабліва там, дзе доступ да інтэрнэту прадастаўляецца дзяржаўнымі кампаніямі, такую інфармацыю атрымаць вельмі проста. Тады ў Сары будуць праблемы.

Існуе шэраг спосабаў, як Сара можа захаваць ананімнасьць, карыстаючысі інтэрнэтам. Як правіла, чым у большай бясьпецы хоча быць чалавек, тым больш працы яму давядзецца правесьці. Сары, і кожнаму іншаму чалавеку, што хоча займацца блогінгам ананімна, неабходна вызначыцца, наколькі вялікая яе (яго) параноя, перш чым вырашыць, колькі намаганьняў прыкласьці да таго, каб захаваць сваю ананімнасьць. Як вы пабачыце далей, некаторыя стратэгіі захаваньня ананімнасьці патрабуюць шмат тэхнічных ведаў і працы.

КРОК 1 – ПСЭЎДАНІМЫ

Самы просты спосаб, каб забясьпечыць ананімнасьць Сары - гэта выкарыстоўваць бясплатныя інтэрнэт-пошту і блогавую плятформу па-за межамі краіны, у якой яна жыве. (Карыстацца платнымі паслугамі для электроннай пошты і інтэрнэту ня варта, таму што па нумары рахунка ці крэдытнай карты можна вызначыць імя карыстальніка). Сара можа стварыць сабе новае імя – псэўданім, якім будзе карыстацца ў сеціве. І калі міністар знойдзе яе блог, ён пабачыць імя аўтара: "Y.N.Ymous" і яго электронны адрас anonymous.whistleblower@hotmail.com.

Вось некарорыя з правайдэраў бясплатных паштовых паслугаў:
Hotmail
Yahoo
Hushmail – бясплатная пошта з добрай крыптаграфічнай абаронай

Некаторыя з правайдэраў бясплатнага хостынгу для блогаў:
Blogsome – бясплатныя WordPress блогі
Blogger
Seo Blog

Аднак тут паўстае праблема стратэгіі. Калі Сара падпісваецца на бясплатную электронную пошту ці бясплатную блогавую плятформу, уэб-сэрвэр, які яна выкарыстоўвае, рэгіструе яе IP адрас. Калі з дапамогай гэтага IP адрасу яе адсочаць – калі яна карыстаецца дамашнім ці працоўным кампутарам – і калі кампанію, што прапануе паслугі пошты ці блогінгу прымусяць паведаміць гэтую інфармацыю, то Сару лёгка знойдуць. Прымусіць большасьць кампаній, што прапануюць паслугі па карыстаньні сецівам, выдаць такую інфармацыю ня так проста. Напрыкалад, каб прымусіць Hotmail раскрыць IP адрас, якім карысталася Сара пры падключэньні, міністру, хутчэй за ўсё, спатрэбіцца спэцыяльны дазвол, па які, магчыма, давядзецца зьвярнуцца да праваахоўных органаў ЗША. Але Сара, магчыма, не захоча рызыкаваць, калі ўлады ў яе краіне могуць пераканаць інтэрнэт-кампаніі, паслугамі якіх яна карысталася, паведаміць інфармацыю пра яе.

КРОК 2 – АГУЛЬНАДАСТУПНЫЯ КАМПУТАРЫ

Каб захаваць ананімнасьць, Сара можа займацца блогінгам на кампутарах, якімі карыстаецца вялікая колькасьць людзей. Зарэгістраваць сваю пошту ці блог яна можа з кампутара ў інтэрнэт-кавярні, бібліятэцы ці ва ўнівэрсытэцкай інтэрнэт-лябараторыі. Калі міністар даведаецца IP адрас аўтара нататкаў ці камэнтароў, ён пабачыць, што паведамленьне дасланае з інтэрнэт-кавярні з кампутара, на якім магло працаваць невядома колькі людзей.

У гэтай стратэгіі таксама ёсьць свае слабыя месцы. Напрыклад, калі ў інтэрнэт-кавярні ці кампутарнай лябараторыі фіксуюецца, хто і ў які час карыстаўся якім кампутарам. У такім выпадку Сару лёгка знайсьці. Ёй ня варта прыходзіць у лябараторыю ўначы, калі там нікога няма, таму што лябарант лёгка яе запомніць. Ёй трэба часта мяняць інтэрнэт-кавярні. Калі

міністар высьветліць, што ўсе паведамленьні дасланыя з інтэрнэт-кавярні "Joe's Beer and Bits" з Мэйн стрыт , ён можа пачаць сачыць за кавярняй і знойдзе Сару.

КРОК 3 – АНАНІМНЫЯ ПРОКСІ-СЭРВЭРЫ

Сары надакучыла хадзіць у інтэрнэт-кавярню кожны раз, калі ёй трэба абнавіць блог. З дапамогай суседа-кампутаршчыка яна атрымала доступ да інтэрнэту праз ананімны проксі-сэрвэр з дамашняга кампутара. Цяпер, калі яна карыстаецца электроннай поштай ці займаецца блогінгам, яна пакідае IP адрас проксі-сэрвэра, а не адрас дамашняга кампутара, і мінстру будзе вельмі цяжка яе знайсьці.
Па-першае, яна знаходзіць у пошукавіку Google сьпіс проксі-сэрвэраў ("proxy server") і выбірае проксі-сэрвэр са сьпісу publicproxyservers.com.list, пазначаны надпісам "high anonymity" ("высокая ступень ананімнасьці"). Яна выпісвае са сьпісу IP адрас проксі і порта.

Вось некалькі надзейных сьпісаў адкрытых проксі-сэрвэраў:

- publicproxyservers.com – ананімныя і неананімныя проксі-сэрвэры;
- Samair (http://www.samair.ru/proxy/) – выключна ананімныя проксі-сэрвэры, а таксама інфармацыя пра проксі-сэрвэры, якія падтрымліваюць SSL;
- Rosinstrument proxy database (http://tools.rosinstrument.com/proxy/) – пошук па базе дадзеных проксі-сэрвэраў).

Потым Сара пераходзіць у разьдзел "preferences" свайго ўэб-пошукавіка. У разьдзелах "general", "network" ці "security" (звычайна) яна знаходзіць опцыю атрыманьня доступу да інтэрнэту праз проксі-сэрвэр. (У пошукавіку Firefox гэтая опцыя знаходзіцца пад Preferences – General - Connection Settings).

Сара ўключае "ручную настройку проксі-сэрвэра ("manual proxy configurations"), уводзіць IP адрас проксі-сэрвэра і порта ў палі для HTTP proxy і SSL proxy і захоўвае свае парамэтры. Яна перазагружае свой браўзэр і пачынае працаваць у інтэрнэце.

Сара заўважае, што сувязь запаволілася. Гэта адбываецца таму, што кожная старонка, на якую яна дае запыт, загружаецца абыходным шляхам. Замест непасрэднага падключэньня да hotmail.com, кампутар злучаецца з проксі-сэрвэрам, і той падключаецца да Hotmail. Старонка, якую Hotmail дасылае Сары, спачатку ідзе на проксі-сэрвэр, а толькі потым да Сары. Яна таксама заўважае, што ўзьніклі цяжкасьці з доступам да ўэб-сайтаў, асабліва да тых, якія патрабуюць рэгістрацыі. Але затое яе IP адрас невядомы правайдэру.

Можна правесьці з проксі-сэрвэрамі цікавы экспэрымэнт: зайдзіце на noreply.org – папулярны сайт, які займаецца перасылкай ("remailer"). На маніторы зьявіцца прывітаньне з вашым IP адрасам: "Hello pool-151-203-182-212.wma.east.verizon.net 151.203.182.212, pleased to meet you".

Цяпер ідзіце на anonymizer.com , які дазваляе бачыць некаторыя ўэб-старонкі праз ананімны проксі. У акно ў правым верхнім куце старонкі ўвядзіце URL для http://www.noreply.org (ці проста націсьніце на спасылку [http://anon.free.anonymizer.com/http://www.noreply.org]. Вам стане зразумела, што noreply.com цяпер лічыць, што вы прыйшлі з vortex.anonymizer.com.(Anonymizer – гэта добры спосаб, каб праверыць проксі-сэрвэры, не зьмяняючы парамэтры ў настройцы вашага браўзэра, але гэта не працуе з больш дасканалымі сэрвэрамі, такімі, як webmail ці weblogging).

І, нарэшце, выконвайце інструкцыі, прыведзеныя вышэй, каб настроіць свой уэб-браўзэр на выкарыстаньне ананімнага проксі-сэрвэра, пасьля чаго наведайце noreply.org, каб даведацца, ці зафіксаваў ён ваш IP адрас.

На жаль, проксі-сэрвэры таксама недасканалыя. Калі ў краіне, дзе жыве Сара, дзейнічаюць законы, якія абмяжоўваюць карыстаньне інтэрнэтам, многія карыстальнікі

будуць выкарыстоўваць проксі-сэрвэры, каб атрымаць доступ да сайтаў, заблякаваных уладамі. Улады могуць у адказ заблякаваць найбольш папулярныя проксі-сэрвэры. Карыстальнікі будуць пераходзіць да новых проксі-сэрвэраў, якія ўлады таксама праз нейкі час заблякуюць, і так па крузе. Праз гэта на пошукі і зьмены проксі-сэрвэраў можна згубіць вельмі шмат часу. Сара можа мець іншую праблему, калі яна адна з нямногіх у сваёй краіне, хто карыстаецца паслугамі проксі-сэрвэраў. Калі яе блог абнаўляецца з аднаго і таго ж проксі-сэрвэра, і калі міністру ўдасца атрымаць рэгістрацыйныя запісы ад усіх інтэрнэт-праваўдэраў (ISPs), што дзейнічаюць у краіне, ён зможа высьветліць, што кампутар Сары – адзін зь нямногіх кампутараў, што зьвязваліся з канкрэтным проксі-сэрвэрам. Ён ня зможа даказаць, што Сара карысталася проксі-сэрвэрам, каб дасылаць абнаўленьні на блог, але ён можа зрабіць высновы, што калі проксі-сэрвэр выкарыстоўвалі, каб даслаць абнаўленьне на блог, і што Сара – адна зь нямногіх людзей у краіне, што карысталіся гэтым проксі-сэрвэрам, то яна – аўтарка гэтага блогу. Таму Сары трэба карыстацца папулярнымі ў яе краіне проксі-сэрвэрамі і часта мяняць іх.

КРОК 4 – ГЭТЫМ РАЗАМ УСЁ НАДЗЕЙНА!

Сара пачынае баяцца, што проксі-сэрвэры, якімі яна карыстаецца, яе выдадуць. Што, калі міністар прымусіць апэратара проксі-сэрвэра (дасьць яму хабар ці націсьне на яго з дапамогай закона) фіксаваць, хто ў яго краіне карыстаецца проксі-сэрвэрам, а таксама якія сайты гэтыя людзі наведваюць. Сара спадзяецца, што адміністратар проксі-сэрвэра яе абароніць, але яна нават ня ведае, хто ён такі. Адміністратар можа нават і ня ведаць, што яна карыстаецца проксі-сэрвэрам, але проксі-сэрвэры часта адчыняюцца выпадкова.

У Сары ёсьць сябры ў Канадзе (у гэтай краіне інтэрнэт не цэнзуруецца так, як у яе на радзіме), якія могуць пагадзіцца дапамагаць ёй весьці блог, захоўваючы яе ананімнасьць. Сара тэлефануе свайму сябру і просіць, каб ён усталяваў на сваім кампутары "Circumventor". "Circumventor" – гэта адзін зь дзясяткаў проксі-сэрвэраў, якія вы можаце ўстляваць на свой кампутар. Гэта дазволіць іншым людзям выкарыстоўваць ваш кампутар у якасьці проксі-сэрвэра.

Джым, сябра Сары, загружае Circumventor (http://www.peacefire.org/circumventor/simple-circumventor-instructions.html) з Peacefire.org і ўсталёўвае яго на сваю Windows сыстэму. Гэта зрабіць няпроста: яму трэба ўсталяваць Perl, потым OpenSA і толькі пасьля іх Circumventor. Акрамя таго, трэба, каб кампутар Джыма увесь час быў падключаны да інтэрнэту, каб Сара магла выкарыстоўваць яго як проксі-сэрвэр, і каб яна не прасіла Джыма кожны раз, калі ёй трэба даслаць матэрыял, падключыцца да інтэрнэту. Джым усталёўвае праграмнае забесьпячэньне, тэлефануе Сары на мабільны тэлефон і паведамляе URL, якім яна будзе карыстацца, каб падключыцца да інтэрнэту ці абнавіць свой блог з дапамогай проксі-сэрвэра Джыма. Гэта зручна яшчэ і тым, што Сара можа карыстацца проксі-сэрвэрам Джыма як дома, так і ў інтэрнэт-кавярні, і ёй ня трэба нічога мяняць у сваім кампутары.

Сара, безумоўна, вельмі ўдзячная Джыму за дапамогу, але тут, усё ж, існуе адна арганізацыйная праблема. Кампутар Джыма (які працуе з сыстэмай Windows) часта перазагружаецца. Кожны раз, калі гэта адбываецца, правайдэр (ISP) прысвойвае машыне новы IP адрас і проксі-сэрвэр перастае працаваць для Сары. Джыму трэба зьвязвацца з Сарай зноўку, каб паведаміць новы IP адрас. Гэта нязручна і дорага. Сару непакоіць і тое, што калі яна доўгі час будзе карыстацца нейкім адным IP адрасам, яе правайдэр можа паддацца ціску з боку ўладаў і заблякаваць гэты адрас.

КРОК 5 – ЦЫБУЛІННАЯ МАРШРУТЫЗАЦЫЯ ПРАЗ TOR (ONION ROUTING THROUGH TOR)

Джым прапануе Сары паэкспэрымэнтаваць з Tor – адносна новай сыстэмай, якая забясьпечвае высокую ступень ананімнасьці карыстальнікам інтэртэту. "Цыбулінная маршрутызацыя" ("onion routing") падымае на новы ўзровень складанасьці ідэю проксі-сэрвэраў (кампутар, якія дзейнічае ад вашага імя). Кожны запыт, зроблены праз сетку "цыбуліннай маршрутызацыі", праходзіць празь некалькі дадатковых кампутараў (якіх можа

быць ад двух да дваццаці). У выніку вельмі цяжка прасачыць, зь якога кампутара быў дасланы запыт.

Кожны крок у ланцугу "цыбуліннай маршрутызацыі" зашыфраваны. Дзякуючы гэтаму ўладам у краіне, дзе жыве Сара, будзе цяжэй адсачыць яе блог. Болей таго, кожны кампутар у ланцугу ведае толькі бліжэйшых суседзяў. Іншымі словамі, маршрутызатар B ведае, што адтрымаў запыт на ўэб-старонку ад маршрутызатара A, і што яму неабходна перадаць запыт маршрутызатару C. Але і сам запыт зашыфраваны – маршрутызатар B насамрэч ня ведае, што гэта за старонка, на якую Сара даслала запыт, ці які маршрутызатар апошні ў ланцугу.

Ведаючы пра складанасьць тэхналёгіі, Сара прыемна зьдзіўленая лёгкасьцю ўсталяваньня сыстэмы "цыбуліннай маршрутызацыі" Tor (http://tor.eff.org/docs/tor-doc-win32.html.en). Яна загружае праграму, якая ўсталёўвае Tor на яе кампутар, потым загружае і ўсталёўвае Privoxy – проксі-сэрвэр, які працуе з Tor і мае дадатковую выгоду таму што аўтаматычна прыбірае рэкляму з уэб- старонак, якія праглядае Сара.

Пасьля ўсталяваньня праграмнага забесьпячэньня і перазагрузкі кампутара Сара заходзіць на noreply.org і бачыць, што яна пасьпяхова "замаскаваная" сыстэмай Tor – noreply.org думае, што яна падключаецца з Гарвардзкага ўнівэрсытэта. Сара перазагружае кампутар - зараз noreply думае, што яна ў Нямеччыне. Сара робіць выснову, што Tor з кожным запытам зьмяняе яе адрас, дапамагаючы ёй захаваць ананімнасьць.

Аднак гэта мае некалькі непрыемных наступстваў. Калі Сара падключаецца да Google праз Tor, пачынаюць пераключацца мовы. Адзін пошук – на ангельскай мове, другі – на японскай, далей на нямецкай, дацкай ці галяндзкай – усё гэта на працягу некалькіх хвілін. Сара ня супраць вывучыць новую мову, але яе непакояць іншыя наступствы. Сары падабаецца пісаць для Wikipedia, але высьвятляецца, што Wikipedia блякуе яе спробы рэдагаваць артыкулы, калі яна карыстаецца Tor.

Выглядае, што з Tor – тыя ж самыя праблемы, што і зь іншымі проксі-сэрвэрамі. Хуткасьць працы ў інтэрнэце запавольваецца, у параўнаньні з працай бяз проксі-сэрвэраў. Сара пачынае карыстацца Tor толькі калі хоча даслаць абнаўленьне на блог ці наведаць забаронены сайт. Зноўку ж яна прывязаная да дамашняга кампутара, таму што вельмі цяжка ўсталяваць Tor на кампутары грамадзкага карыстаньня.

Але болей за ўсё Сару непакоіць тое, што час ад часу Tor перастае працаваць. Відавочна, што яе правайдэр блякуе некаторыя маршрутызатары "цыбуліны" – Tor спрабуе злучыцца з заблякаваным маршрутызатарам, але нават пасьля некалькіх хвілін чаканьня патрэбная старонка так і не адчыняецца.

КРОК 6 – MIXMASTER, INVISIBLOG І GPG

Безумоўна, праблему блогінгу можна вырашыць і без выкарыстаньня проксі-сэрвэраў, нават такіх дасканалых, як Tor.

Пасьля шматлікіх кансультацый зь мясцовымі кампутарнымі спэцыялістамі Сара спрабуе новы варыянт: invisiblog (http://www.invisiblog.com/). Гэта сайт ананімнай групы аўстралійцаў, які мае назву vigilant.tv – створаны параноікамі і для параноікаў. На Invisiblog немагчыма дасылаць свае матэрыялы праз сеціва (як гэта робіцца з большасьцю блогінгавых сэрвэраў), але па электроннай пошце адмысловага фармату, праз рымэйлерную сыстэму MixMaster, якая мае крыптаграфічны подпіс.

Сара зрабіла некалькі спробаў, перш чым зразумела сэнс апошняга сказа. У рэшце рэшт, яна ўсталявала GPG (http://www.gnupg.org/) - GNU вэрсію "Pretty Good Privacy" ("Дастатковая ступень ананімнасьці"). Гэта сыстэма шыфроўкі з адкрытым ключом (http://en.wikipedia.org/wiki/Public-key_cryptography).

Коратка гэта можна патлумачыць наступным чынам: шыфроўка з "адкрытым" ключом – гэты тэхніка, якая дазволіць Сары дасылаць паведамленьні нейкай асобе, якія можа прачытаць толькі яна; яна не паведамляе вам свой "закрыты"ключ, каб вы не змаглі прачытаць паведамленьні, якія іншыя людзі дасылаюць ёй. Шыфроўка з "адкрытым" ключом таксама дазваляе "ставіць лічбавы подпіс" пад дакумэнтам, які амаль немагчыма падрабіць.

Сара стварае пару ключоў, якія яна будзе выкарыстоўваць, дасылаючы абнаўленьні на свой блог і падпісваючыся пад нататкамі з дапамогай "закрытага" ключа. Блог-сэрвэр зможа з дапамогай яе "адкрытага" ключа спраўдзіць, ці нататкі даслала менавіта яна, пасьля чаго разьмесьціць іх на блогу. (глядзіце таксама разьдзел "Як забясьпечыць прыватнасьць электроннай пошты".)

Потым Сара ўсталёўвае MixMaster – паштовую сыстэму, створаную для таго, каб хаваць паходжаньне электроннага паведамленьня. MixMaster выкарыстоўвае ланцуг ананімных рымэйлераў – кампутарных праграм, якія прыбіраюць усю апазнавальную інфармацыю з электроннага паведамленьня і перасылаюць яго адрасату. Гэта робіцца для забесьпячэньня высокай ступені ананімнасьці. Калі выкарыстоўваецца ад двух да дваццаці рымэйлераў, вельмі цяжка адсачыць паведамленьне, нават калі адзін ці болей рымэйлераў "падкупленыя" і запісваюць інфармацыю пра аўтара паведамленьня. Для таго, каб "пабудаваць" MixMaster, Сары трэба сабраць яго першапачатновы код. У гэтай справе ёй спатрэбіцца дапамога кампутарнага спэцыяліста.

Сара дасылае першае MixMaster паведамленьне, разам з "адкрытым" ключом, на Invisiblog. Invisiblog выкарыстоўвае гэта, каб стварыць новы блог з мудрагелістай назвай "invisiblog.com/ac4589d7001ac238" – ланцуг з шаснаццаці апошніх байтаў GPG ключа Сары. Наступныя паведамленьні Сара дасылае на Invisiblog такім чынам: піша тэкст паведамленьня, падпісвае яго сваім "адкрытым" ключом і адпраўляе яго праз MixMaster.

Хуткасьць блогінгу пры гэтым значна запавольваецца. Паколькі MixMaster перанакіроўвае паведамленьне (заблытавае шляхі), паведамленьне ідзе да сэрвэраў ад двух гадзін да двух дзён. Сары таксама трэба быць асьцярожнай і не заходзіць на блог у якасьці наведніка занадта часта, бо ў такім выпадку яе IP адрас зьявіцца ў сьпісе частых наведнікаў блогу, з чаго можна зрабіць выснову, што яна - аўтарка блогу. Але Сара супакойвае сябе тым, што ўладальнікі Invisiblog ня ведаюць, хто яна.

Асноўная праблема з сыстэмай Invisiblog – гэта тое, што яе выкарыстаньне вельмі складанае для большасьці людзей. Для іх усталяваньне GPG – гэта вялікая праблема, і ім таксама цяжка зразумець усе складанасьці "адкрытага" і "закрытага" ключоў. Нават сыстэмы крыптаграфіі, створаныя для звычайных карыстальнікаў, такія, як, напрыклад, Ciphire, не такія простыя. У выніку, вельмі мала людзей, нават сярод тых, каму гэта неабходна, выкарыстоўваюць шыфраваньне для большай часткі сваёй электроннай карэспандэнцыі.

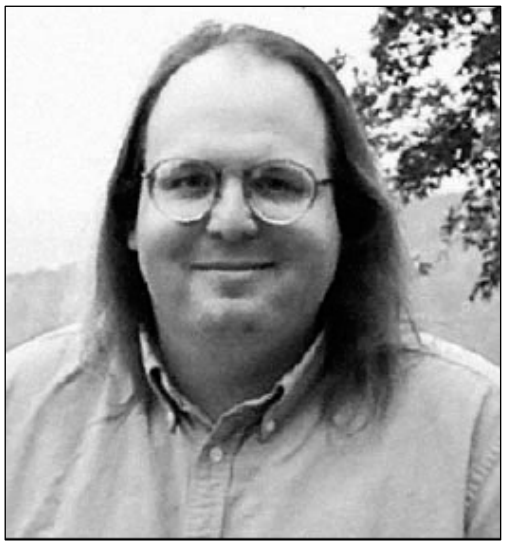
MixMaster – тэхнічна цяжкая задача для большасьці карыстальнікаў. Карыстальнікі Windows могуць зьвярнуцца да раньняй DOS-вэрсыі праграмы, якую можна загрузіць з: http://prdownloads.sourceforge.net/mixmaster/mix204b46.zip?download. Я загрузіў і паспрабаваў яе, але яна чамусці не працуе... магчыма, маё паведамленьне дагэтуль перасылаецца ад рымэйлера да рымэйлера. Таму, хто хоча паспрабаваць больш новую вэрсію ці праграму на Linux ці Mac, трэба пісаць праграмы самім, а гэтая задача не пад сілу нават шмат якім вопытным карыстальнікам. Магчыма, Invisiblog стане больш даступным, калі пачне прыймаць паведамленьні ад рымэйлераў, даступных праз сеціва, напрыклад, такіх, як riot.eu.org. Але пакуль наўрадці ён дапаможа тым, каму ён сапраўды патрэбен.

У краінах з рэпрэсіўным рэжымам існуе яшчэ адна праблема з моцным шыфраваньнем. Калі ўлады канфіскуюць кампутар Сары і знойдуць яе "закрыты" ключ, гэта будзе сур'ёзным доказам таго, што Сара - аўтарка "падрыўных" матэрыялаў на блогу. У краінах, дзе шыфраваньне шырока не выкарыстоўваецца, проста адправіць паведамленьне праз

MixMaster, дзе яно моцна шыфруецца, можа быць дастаткова для таго, каб за дзейнасьцю Сары ў інтэрнэце пачалі сачыць.

ЯКАЯ АПТЫМАЛЬНАЯ СТУПЕНЬ АНАНІМНАСЬЦІ? ДЗЕ ТРЭБА СПЫНІЦЦА?

Ці падыходзіць вам рашэньне Сары: атрымаць дадатковыя веды пра шыфраваньне і праграмнае забесьпячэньне, каб выкарыстоўваць MixMaster? Ці, можа, вам дастаткова скамбінаваць крокі 1-5, каб займацца блогінгам ананімна? Адназначнага адказу няма. Пры выбары спосабу, з дапамогай якога захоўваць ананімнасьць, неабходна ўлічваць мясцовыя ўмовы, вашу тэхнічную падрыхтоўку, а таксама ступень вашай параноі. Калі вы лічыце, што весьці блог рызыкоўна, і што вам пад сілу ўсталяваць Tor, то гэта вельмі добрае рашэньне праблемы.



І памятайце: ня варта падпісваць нататкі на блогу вашым сапраўдным імем!

Этан Цукерман – супрацоўнік Цэнтра імя Бэркмана "Інтэрнэт і грамадзтва" на юрыдычным факультэце Гарвардзкага ўнівэрсытэта (the Berkman Center for Internet and Society at Harward Law School). Тэма яго дасьледаваньняў – адносіны паміж грамадзянскай журналістыкай і традыцыйнымі мэдыямі, галоўным чынам, у разьвіцьцёвых краінах. Ён – заснавальнік і былы дырэктар "Geekcorps" – НДА, якая праводзіць трэнінгі па авалоданьні кампутарнымі тэхналёгіямі ў разьвіцьцёвых краінах. Этан Цукерман – адзін з заснавальнікаў хостынгавай кампаніі Tripod.

KAMUNIKA.TV