ЯК ЗАБЯСЬПЕЧЫЦЬ **КАНФІДЭНЦЫЙНАСЬЦЬ** ЭЛЕКТРОННАГА ЛІСТАВАНЬНЯ

Людовік Пьера (Ludovic Pierrat)

У большасьці краін улады маюць магчымасьці праглядаць электонную пошту. У краінах з рэпрэсіўным рэжымам "кібэрпаліцыя" выкарыстоўвае гэтыя магчымасьці, каб адсочваць і арыштоўваць палітычных апанэнтаў; многія палітычныя лідэры патрапляюць за краты за адпраўленьне, ці нават перасылку электронных паведамленьняў. Адзін палітычны дысыдэнт на Мальдывах быў асуджаны на 15 год турэмнага зьняволеньня за электроннае ліставаньне з праваабарончай арганізацыяй "Amnesty International". Карыстальнік інтэрнэту ў Сырыі зь лютага 2003 году знаходзіцца ў турме за перасылку бюлетэня, што распаўсюджваецца па электроннай пошце.

Такім чынам, я прапаную некаторыя парады, як забясьпечыць канфідэнцыйнасьць электроннай пошты.

Карыстаньне адрасам электроннай пошты, выдадзеным вашым інтэрнэт-правайдэрам (ISP), напрыклад, AOL, Wanadoo ці Free, або адрасам, выдадзеным кампаніяй, у якой вы працуеце, не гарантуе канфідэнцыйнасьці электроннага ліставаньня. Уладальнікі сетак, праз якія праходзяць вашыя паведамленьні, могуць зь лёгкасьцю іх перахопліваць. Калі ўлады ў нейкай краіне пачынаюць сачыць за карыстальнікамі інтэрнэту, то звычайна атрымліваюць доступ да іх электроннай карэспандэнцыі праз правайдэраў.

Адрасы ўэб-пошты, такія, як Yahoo! ці Hotmail, больш надзейныя, таму што тут не выкарыстоўваюцца сэрвэры мясцовых правайдэраў. Каб кантраляваць такое ліставаньне, трэба неяк "прабіцца" ў сыстэму ці перахопліваць пасланьні падчас іх перасылкі, што тэхнічна больш складана. Нажаль, гэтая перавага вельмі адносная, таму што кампутарныя спэцыялісты з паліцыі ці хакеры ўсё адно могуць праглядаць вашую пошту.

Шыфраваньне (абарона пошты з дапамогай коду) – асноўны спосаб рэальна забясьпечыць канфідэнцыйнасьць вашых паведамленьняў. Ёсьць два спосабы шыфраваньня:

КЛЯСЫЧНАЕ ШЫФРАВАНЬНЕ

Эн і Майкл хочуць весьці сакрэтнае ліставаньне. Яны дамаўляюцца пра коды зашыфроўкі і расшыфроўкі, а таксама пра ключ, і пачынаюць ліставаньне.

З гэтым спосабам можа паўстаць праблема, калі трэцяя асоба перахопіць паведамленьне, у якім Эн і Майкл абменьваюцца ключамі. Акрамя таго, што іх ліставаньне будуць чытаць, ім яшчэ могуць дасылаць і фальшывыя паведамленьні. Такім чынам, Эн і Майклу трэба абмяняцца ключамі так, каб ніхто гэтага ня ўбачыў, напрыклад, пры асабістай сустрэчы.

АСЫМЭТРЫЧНАЕ ШЫФРАВАНЬНЕ

Найлепшы спосаб вырашэньня праблемы канфідэнцыйнасьці – гэта "асымэтрычнае" шыфраваньне. Для гэтага патрэбныя два ключы – адзін для зашыфроўкі, другі – для

расшыфроўкі. Ключом для зашыфроўкі ("адкрытым ключом") можна абмяняцца праз інтэрнэт не баючыся, таму што зь яго дапамогай немагчыма расшыфраваць пасланьне. Ключ для расшыфроўкі ("сакрэтны" ці "закрыты" ключ) не абмяркоўваецца.

Пры асымэтрычным шыфраваньні Эн мае два ключы (адкыты, які яна паведамляе, і закрыты, якога ніхто ня ведае). Эн дасылае свой ключ Майклу. З дапамогай гэтага ключа Майкл зашыфроўвае свае пасланьні да Эн. Толькі Эн з дапамогай свайго сакрэтнага ключа можа расшыфраваць пасланьні Майкла. Майкл мае свае два ключы. Ён, у сваю чаргу, дасылае Эн свой адкрыты ключ. Такім чынам, Эн адказвае на пасланьні Майкла, не турбуючыся пра канфідэнцыйнасьць паведамленьняў.

Але паколькі адкрыты ключ перадаецца праз інтэрнэт без нейкай спэцыяльнай абароны, лепей разам зь яго аўтарам яго ўзгадніць. Кожны ключ мае "адбіткі пальцаў" (кароткі набор сымбаляў, знакаў), якія можна перадаць асабіста ці па тэлефоне.

Трэцяя асоба можа замяніць няўзгоднены ключ на фальшывы, тады шыфраваньне згубіць усялякі сэнс. Надзейнасьць асымэтрычнага шыфраваньня цалкам залежыць ад абароны сакрэтнага ключа, а таксама ад праверкі аўтэнтычнасьці адкрытага ключа асобы, зь якой вядзецца ліставаньне.

OpenPGP (Open Pretty Good Privacy) – гэта стандартны спосаб асымэтрычнага шыфраваньня. Найбольш папулярнае праграмнае забесьпячэньне для стварэньня і выкарыстаньня двух ключоў (адкрытага і закрытага), а таксама кіраваньня адкрытымі ключамі тых, хто лістуецца, - гэта GnuPG (GNU Privacy Guard), якое можна выкарыстоўваць як з паштовымі праграмамі (такімі, як Thunderbird і Outlook), так і з уэб-поштай і тэрміновым ліставаньнем.

Праграму GnuPG можна загрузіць з сайта www.gnupg.org

Спэцыяльную вэрсію для Windows можна знайсьці на www.winpt.org

Людовік Пьера – кампутарны інжынэр, узначальвае кампанію "Wa Company", якая займаецца кансультаваньнем і вытворчасьцю ў галіне інфармацыйных тэхналёгій.

КАМУНІКАТ.org