Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

Res millor que el codi obert ben analitzat (6936 lectures)

Per **Benjamí Villoslada**, ***Benjami*** (http://weblog.bitassa.net)

Creado el 22/10/2004 15:01 modificado el 22/10/2004 15:01

> *Al seu nou bloc[1], Bruce Schneier respon una pregunta que sorgeix sovint en parlar de seguretat: Els programes oberts són més segurs que els tancats? Diu que quan el codi obert és analitzat, no hi ha res millor.*

El pinyol de l'assumpte està al voltant de la paraula **anàlisi**. Per saber quina és la seguretat d'un producte, cal que experts analitzin el codi.

En el cas dels programes tancats, Schneier diu que cal llogar experts per que l'analitzin. Si es tracta de programari obert, el fet de publicar el codi forma part de la cosa. Així, la revisió s'aconsegueix amb el fet natural de publicar el codi i esperar que algú el revisi.

On està la diferència que fa el codi obert ben analitzat sigui millor?

En els dos entorns, tancat i obert, la revisió és una feinada. Això explica que molts programes oberts siguin insegurs. Simplement sol passar que cap expert n'ha fet una revisió rigorosa. El mateix es pot dir de molts programes tancats.

En el cas del codi obert, per aconseguir un anàlisi primer cal captar l'interès dels experts amb un bon projecte. És el que des de sempre ha estimulat l'intel·lecte de tots els experts de qualsevol ram. Els seus estudis es podran publicar i sotmetre a revisió per iguals, un ingredient bàsic del mètode científic. Se'n beneficia tota la comunitat d'experts i més endavant els usuaris. Practicar el mètode científic també és un bon incentiu.

Però si es vol analitzar un producte tancat, caldrà aconseguir permís per poder veure i analitzar el codi. La feina estarà pagada o no, però en qualsevol cas hi haurà un contracte signat (Non-Disclosure Agreement, NDA) que prohibirà publicar el codi, la matèria primera de l'anàlisi. Si altres experts tenen dubtes, sense codi no podran fer la revisió per iguals. Per aconseguir-lo caldrà que signin més contractes NDA i la història es repetirà. Això si els accepten; no és tant fàcil com baixar el codi d'un projecte obert i analitzar-lo sense haver de demanar res ni passar comptes amb ningú --detall que, de passada, contribueix a la imparcialitat dels anàlisi. Per tot plegat sol passar que l'empresa paga experts seleccionats a canvi d'un anàlisi que mai no surt completament de les seves portes. Només es solen publicar les conclusions i sovint amb propòsits publicitaris.

En definitiva, no es pot dir que un programa tancat o obert és segur fins que experts no l'han revisat. El model tancat dificulta la publicació d'anàlisi amb garanties científiques.

Per tot plegat, no és casualitat que a l'hora de dir programes que estan ben analitzats, Bruce Schneier posi com a exemple Linux, Apache i OpenBSD. Cap d'aquests té el codi tancat i per això diu que quan el codi obert és correctament analitzat, no hi ha res millor: *«When open-source code is properly analyzed, there's nothing better»*.

Aprofito per recomanar la subscripció[2] al seu Crypto-Gram Newsletter.

(Article original[3])

Lista de enlaces de este artículo:

1. http://www.schneier.com/blog/archives/2004/10/schneier_securi.html
2. http://www.schneier.com/crypto-gram.html

3. http://weblog.bitassa.net/arxiu/2004/10/22/45/

E-mail del autor: benjami _ARROBA_ bitassa.com