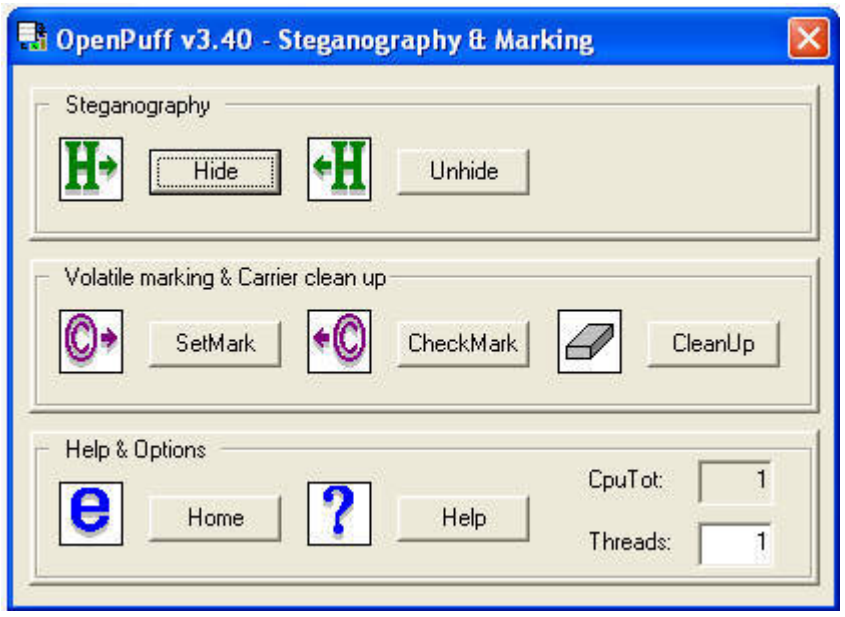
Steganographie

von realasmodis @ 2012-04-15 – 19:40:27

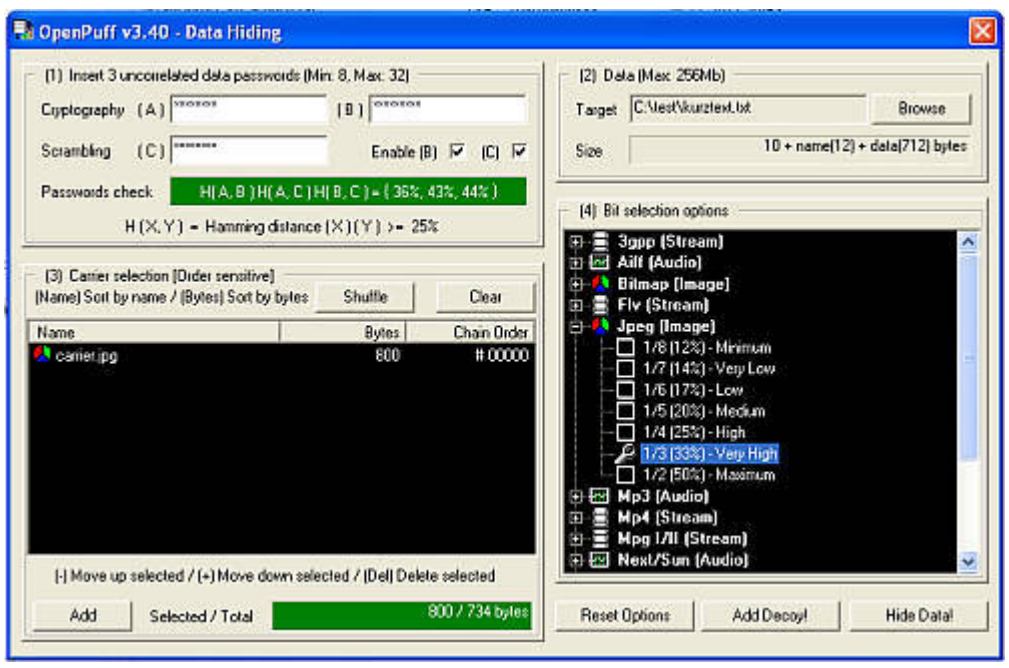
Im Beitrag "Ausspioniert!" hatte ich mich ja schon mal dazu geäußert, was ich von den Bespitzelungspraktiken unserer Sicherheitsbehörden halte - auch wenn das alles nur meinem eigenen Schutz dient: **Danke, lieber Staat, aber ich passe ganz gerne selbst auf mich auf und brauche daher keinen Big Brother!** Jedenfalls erreichten mich in Folge ein paar ein Mailanfragen dazu, wie ich es selbst denn mit der Verschlüsselung von Mails halte. Ganz einfach: Ich verschlüssele NICHT. Weil ich es kontraproduktiv finde. Wenn wir schon nach Kräften ausspioniert werden, dann fällt eine verschlüsselte Mail nämlich auf wie ein Leuchtfeuer in finsterster Nacht. Obwohl es mit Portable PGP, LockNote oder dem Steganosdienst FreeCrypt wirklich recht gute und auch einfach zu bedienende Verschlüsselungsmethoden gibt.

Ich betrachte die Sache etwas anders. Wo versteckt man sich am besten? In einer Menschenmasse. Auf die Weise habe ich auch schon den Schatten eines gewissen "Dienstes" abhängen können, was man hinterher auch zugab. Wie versteckt man also Informationen im Internet? Ganz einfach - in anderen Informationen. In völlig unverfänglichen Bildern, Audiodateien, Streams, Diashows, Filmen, PDF-Texten. Das Verfahren nennt sich Steganographie. Dabei versteckt man eine Datei unsichtbar in einer anderen, möglichst verschlüsselt. Es gibt etliche mehr oder weniger gute Steganographie-Programme und ich habe viele ausprobiert. Unter Windows gefällt mir persönlich das portable OpenPuff am besten und deswegen will ich das hier mal vorstellen.

Die Software kommt als 5,4 MB-ZIP-Archiv. Nach dem Entpacken beansprucht sie rund 10 MB. Gestartet wird das Programm mit "OpenPuffv340.exe". Es folgt ein Fensterchen mit einem Ladebalken "Race Condition Source", danach die Auswahltabelle bzg. Ver- oder Entschlüsselung. "Hide" dient der Verschlüsselung; "Unhide" der Entschlüsselung.



Bleiben wir zunächst bei der Verschlüsselung; dazu wird auf "Hide" geklickt. Das Fenster wechselt; jetzt geht's an's Eingemachte. Vier Schritte sind nötig, als "(1)" bis "(4)" in den vier Fenstern bezeichnet. Das erste Fenster "(1)" verlangt nach der Eingabe von maximal drei Passwörtern. Jedes davon muss mindestens 8 und darf maximal 32 Zeichen umfassen. Werden Zeichenfolgen außerhalb dieses Bereichs eingegeben, dann bleiben sie rot unterlegt und das Programm akzeptiert sie nicht. Ist hingegen alles OK, dann wechselt die Hintergrundfarbe auf grün. Dieser Farbwechsel findet sich übrigens auch in Fenster "(3)" wieder.



In Fenster "(2)" wird die zu versteckende (Text-) Datei - die Quelldatei - ausgewählt; sie darf maximal 256 MB umfassen, sofern die Container- oder Zieldatei, in der versteckt werden soll, groß genug ist. Wie groß die Quelldatei allerdings im jeweiligen Einzelfall sein kann, hängt vom "Container", also von der Datei, in der man verstecken will, ab. Bei 256 MB müsste das schon ein 4-GB-Film sein. OpenPuff ist so komfortabel, das gleich zu berechnen, nämlich in Fenster "(3)". In Fenster "(3)" gibt man die Datei an, in der die Daten versteckt werden sollen. Im Anzeigefeld unter dem Fenster findet sich links die Angabe der maximal versteckbaren und rechts die Angabe der real versteckten Bytes. Wird das in grün dargestellt, dann ist auch alles im grünen Bereich.

Fenster "(4)" schließlich dient der Auswahl des Dateityps - in der o. a. Abbildung habe ich Plain-Text in einem JPG-Container untergebracht, muss also "JPEG (Image)" wählen - und der Wahl des Umfangs der zu versteckenden Daten (hier: "1/3 - Very High"). Zuletzt klickt man auf "Hide Data!" und wählt den Ausgabeordner (der nicht mit dem Ordner identisch sein darf, in dem der unter Fenster "(3)" gewählte Datencontainer sitzt, denn andernfalls bricht die Software zwangsläufig mit einer Fehlermeldung ab). Fertig! Die Größe der Containerdatei sowie ihre Zeit- und Datumseinträge werden durch das Einfügen der zu versteckenden Daten nicht verändert; auch erkennt ein Anti-Steganographie-Tool wie Stegdetect die Manipulation nicht. Das Extrahieren von versteckten Daten geschieht in äquivalenter Form, nur wählt man dazu eben auf dem Eingangsbildschirm "Unhide".

So, und wie funktioniert das jetzt in der Praxis? Man legt sich die zu versteckende Datei zurecht und bspw. ein JPG-Bild. Je größer das ist, desto mehr kann darin versteckt werden. Faustregel dazu (per try and error ermittelt): Rund 0,2% bis max. 0,5% des Speicherbedarfs der Containerdatei, in der die Daten

versteckt werden sollen, darf die zu versteckende Datei umfassen. Und: Ein Kilobyte Plain-Text ist im Druck etwa eine halbe Normseite (die Normseite umfasst maximal 60 Anschläge pro Zeile und 30 Zeilen pro Seite) groß. Notfalls werden die Daten auf mehrere Container verteilt; auch das unterstützt OpenPuff. Die so versteckten Daten übermittelt man als vollkommen unverfängliches Bild per Mail. Oder man legt sie auf einer Webseite ab. Oder bei Facebook. Wie auch immer. Weiß ja außer Absender und Empfänger keiner, was da drin steckt. Der Empfänger erhält jetzt folgende Informationen auf anderem Weg (SMS, Telefonat, Snailmail etc.):

- Welches Steganographieprogramm notwendig ist (nämlich OpenPuff) und
- die drei Passwörter (wenn man denn mit drei PWs verschlüsselt hat).

Er lädt sich das Bild (oder die Bilder oder die Audiodatei oder das PDF oder ...) runter (rechte Maustaste; "Grafik speichern unter ...") und extrahiert mit eben diesen Angaben den darin verborgenen Text. Was zu beachten ist: Nach dem Verstecken des Textes darf die Containerdatei nicht mehr bearbeitet werden, weil eine nachträgliche Bearbeitung unweigerlich zur Zerstörung der Informationen führen würde. Außerdem wäre es vollkommener Blödsinn, dem Empfänger die o. e. Zugangsdaten per Mail zukommen zu lassen (weil man dann auch gleich komplett auf die Verschlüsselung verzichten könnte - andere lesen ja bekanntlich mit). Anzumerken wäre noch, dass OpenPuff gleich eine ganze Handvoll verschiedener und wirklich guter Verschlüsselungsalgorithmen mehr oder weniger simultan anwendet. Man kann den Datenschutz ja vielleicht auch übertreiben ... Ach ja, und ein weiteres Tutorial findet sich bei Youtube.