حماية البريد بالتشفير و التوقيع الرقمي

مقدمة

الكثير من الاشخاص يقومون بإرسال رسائل بريد عالية السرية و هذه الرسائل قد تكون معرضة للتجسس
و التعديل اذا لم تكون محمية بقوة
open pgp و هذه الحماية ممكنة بستخدام معايير
أحد أهم طرق حماية البيانات Pretty Good Privacy أي خصوصية جيدة جداً PGP تعتبر
digital signatures الشخصية الخاصة أو فحص سلامة التوقيع الرقمي
باستخدام خوارزميات موثوقة وآمنة إلى حد بعيد
تعتمد هذه المعايير على وجود ملفان عام وخاص (سري وعلني) يسميان زوجا المفاتيح

(المفتاح العام ترسله للجميع و المفتاح الخاص (سري

كيف يكون التشفير و فك التشفير؟؟

اذا اراد شخص ارسال رسالة لك يقوم بتشفير الرسالة بمفتاحك العلني
و هاذه الرسالة لا يمكن فك تشفيرها الا بمفتاحك السري,

كيف يكون التوقيع؟

التوقيع الرقمي هو طريقة لاثبات صحت مرسل الرسالة
و يتم هذا بخطوتين
* يقوم المرسل ب توقيع(تشفير مع وجود نسخة غير مشفرة) الرسالة بستخدام مفتاحه السري
*يقوم المستلمين بالتحقق من صحت الرسالة و المرسل باستخدام مفتاحك العام
الان نأتي للشرح العملي
من منظمة جنو gpg سوف نستخدم في الشرح برنامج

وهو برنامج قوي مفتوح المصدر يعمل على العديد من انظمة التشغيل
open pgp و يدعم جميع معايير,
هناك العديد من الطرق لستخدام البرنامج و لاكن سوف نشرح طريقة الاستخدام من الطرفية
فالكثير من الاجهزة هي عبارة عن خوادم لا تملك واجهة رسومية

تحميل البرنامج

مثبت مع اغلب توزيعات جنو لينكس gpg يءتي
و اذا كن غير مثبت او اذا كنت تريد تحديثه
نفذ الامر

```
$ sudo apt-get install gpg
```

لتحميل البرنامج على انظمة ويندوس من هاذ الرابط:
http://gpg4win.org/download.html
و لمستخدمين الماك من هاذ الرابط:
http://www.gpgtools.org/installer/index.html

و للتأكد من تنصيب البرنامج نفذ الامر

```
$ gpg --help
```

سوف يظهر لك معلومات عن البرنامج

توليد زوج المفاتيح

لتوليد زوج مفاتيحك(العام و الخاص) نفذ الامر ب الطرفية

$ gpg --gen-key

سوف يسألك بعض الاسئلة لتوليد المفاتيح

gpg (GnuPG) 2.0.22; Copyright (C) 2013 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Please select what kind of key you want:
(1) RSA and RSA (default)
(2) DSA and Elgamal
(3) DSA (sign only)
(4) RSA (sign only)
Your selection? 1

هنا يسألك عن نوع المفتاح النوع الافتراضي هو النوع الاول

نفذ الامر رقم 1 او اضغط على مفتاح الادخال

RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048)

هنا يسألك عن طول المفتاح

كلما زاد طول المفتاح زادت قوته

نفذ الامر طول المفتاح و اضغط على مفتاح الادخال

Please specify how long the key should be valid.
0 = key does not expire
<n> = key expires in n days
<n>w = key expires in n weeks
<n>m = key expires in n months
<n>y = key expires in n years
Key is valid for? (0) 1

هنا يسألك عن عمر المفتاح

نفذ الامر 0 اذا تريد ان يستمر المفتاح للابد

و عدد الايام اذا كنت تريد ان يستمر المفتاح ل عدة ايام فقط n نفذ الامر

و عدد الاسابيع اذا كنت تريد ان يستمر المفتاح ل عدة اسابيع فقط nw نفذ الامر

و عدد الشهور nm نفذ الامر

اذا كنت تريد ان يستمر المفتاح ل عدة شهور فقط

و عدد السنين اذا كنت تريد ان يستمر المفتاح ل عدة سنين ny نفذ الامر

كلما زادة سرية المعلومات المتبادلة قل عمر المفتاح
سوف اختار سنة مناسبة لي
Key expires at Thu 23 May 2015 07:17:55 AM AST
Is this correct? (y/N) y
You need a user ID to identify your key; the software constructs the user ID
from the Real Name, Comment and Email Address in this form:
Real name:
(هنا سوف يسءلك عن اسم صاحب المفتاح(نفذ الامر اسمك
Email address:
(هنا سوف يسءلك عن ايميل صاحب المفتاح(ايميلك
Comment:
.إذا أردت أن تكتب تعليق أو أي شيئ نفذ الامره وإلا اتركه فارغ

You selected this USER-ID:
Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
هنا يظهر لك المعلومات و يسئلك عن صحتها
وضغط على زر الادخال o اذا كان كل شيء تمام نفذ الامر
You need a Passphrase to protect your secret key.
Enter passphrase:
هنا يطلب منك ادخال كلمة سر لحماية المفتاح السري
ادخل الكلمة السرية واضغط على مفتاح الادخال
Repeat passphrase:
اعد كتابة الكلمة السرية
We need to generate a lot of random bytes. It is a good idea to perform some other action (type on the keyboard, move the mouse, utilize the disks) during the prime generation; this gives the random number generator a better chance to gain enough entropy.
+++++
+++++.....++++++
....+++++
...+++++
gpg: key 985C517A marked as ultimately trusted
public and secret key created and signed.
gpg: checking the trustdb
gpg: public key of ultimately trusted key 284D2D7B not found
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0 valid: 2 signed: 0 trust: 0-, 0q, 0n, 0m, 0f, 2u
gpg: next trustdb check due at 2012-05-23
pub 2048R/985C517A 2011-05-24 [expires: 2012-05-23]

Key fingerprint = 0F6B 3FCB C827 2B25 407B 4988 0AAE 1B07 985C 517A
sub 2048R/3E428AF5 2011-05-24 [expires: 2012-05-23]
$
الان ستبدأ عملية توليد المفتاح انتظر حتى تنتهي وحرك الفأرة أو كبر وصغر النوافذ أثناء هذه العملية, إذا انتهت ستعود للطرفيّة.

ادارة المفاتيح

لستعراظ المفاتيح العامة نفذ الامر
$ gpg --list-keys
لستعراظ المفاتيح السرية نكتب
$gpg –list-secret-keys

لتصدير المفتاح العام ل ملف نصي حتا يمكنك ارساله للاشخاص
نفذ الامر
$ gpg --armor --export > pk.txt
ملاحظة pk هو الملف الناتج الذي يحتوي على المفتاح
لستيراد مفتاح عام من ملف مفتاح قمت ب تحميله نفذ الامر
$ gpg --import namekey.txt
namekey.txt استبدل
بسم الملف
حذف المفاتيح
لحذف مفتاح
نفذ الامر
--delete-keys
متبوع باسم صاحب المفتاح او بريده
كما في المثال التالي
$ gpg --delete-keys Friend

gpg (GnuPG) 2.0.22; Copyright (C) 2013 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
pub 1024R/57003613 2011-05-24 Friend <mail@gmail.com>
Delete this key from the keyring? (y/N) y
$

تبادل المفاتيح

لتتمكن من فحص صحة توقيع رقمي لشخص آخر أو أن ترسل له بيانات مشفرة يجب أن تمتلك المفتاحه العام (العلني)، فقط من يمتلك المفتاح الآخر (الخاص أي السري) هو من
يمكنه أن يوقع أو يفك البيانات المشفرة بالمفتاح العام المقابل، هذا يعني أن المفاتيح العامة يجب أن تنشر للآخرين، يمكن أن يتم ذلك بواسطة مرفقات رسالة في البريد
أو 'certserver.pgp.com' الإلكتروني أو بوضعه على أحد خادمات المفاتيح مثل
ويكفي وضعه على أحدها لأنها تحافظ على تحديث بعضها البعض. لنشر 'www.keyserver.net'
على ذلك الخادم استخدم 'mykey' مفتاحك العام المشار له ب
$ gpg --keyserver certserver.pgp.com --send-key mykey
متبوع بالمعرّف الست-عشري على الشكل التالي "--recv-key" ولتحصل على المفتاح العام استعمال:
$ gpg --keyserver certserver.pgp.com --recv-key 0xXXXXXXXX
إذا نزّلت ملف المفتاح العام من الإنترنت أو مرفقات بالبريد يمكنك أن تضيفه إلى سلسلة المفاتيح المحفوظة داخل GPG بواسطة "gpg --import file.gpg".

فقط، أي لا يوجد شخص آخر self-signed يمكن أن يكون المفتاح العام الذي حصلت عليه موقع ذاتياً
عليه الذي يدعي أنه صاحبه هو الذي يشهد على صحته، لا أحد يدعم هذا
الإدعاء عبر توقيعه الرقمي، عليك التحقق من أنه صاحبه الحقيقي من خلال بصمة المفتاح التي تعرضها
وذلك بالاتصال مع صاحبه الأصلي ومطابقتها ،"--fingerprnt" بواسطة
بأية طريقة (وجهاً لوجه، عبر الهاتف، عبر موقع الويب ...إلخ) طالما أنك متأكد أنك تتعامل مع صاحب
المفتاح الحقيقي، إذا كان هذا حصل التطابق يمكنك أن تشهد أنت
فلا يعود مجرد مفتاح موقع ذاتياً، الخيار "--sign-key hiskey" على صحته بتوقيعك بواسطة
يعمل على فحص وعرض التواقيع التي تشهد على صحة هذا المفتاح "--check-sigs"
جربها يجب أن تشاهد بنفسك إضافة للتوقع الذاتي.

تشفير و فك تشفير الرسائل

لتشفير رسالة انسخ محتويات الرسالة في ملف نصي
فلنفترض ان اسم الملف rose.txt
و نفذ الامر
$ gpg --output rose.gpg --encrypt --recipient key rose.txt
سوف ينتج ملف مشفر بإسم rose.gpg
انسخ محتوياته في خدمة البريد في خانة الرسالة
ملاحظة
استبدل key بالمفتاح العام لشخص الذي تريد ارسال الرسالة له

اذا حصلت على ملف او رسالة مشفرة و تريد فك تشفيرها بمفتاحك الخاص نفذ الامر
$ gpg --output file --decrypt file.gpg
سوف يسئلك عن كلمة سر مفتاحك الخاص

بسم الملف file ملاحظة استبدل

التوقيع الرقمي للرسائل

متبوعة باسم الملف الذي "clearsign--" أو "sign--" إذا رغبت في توقع رسالة (أي ملف) استعمال
تريد توقيعه، مخرجات الأول تكون عبارة عن رموز ثنائية (ورموز غير
clear text لهذا في حالة الرسال قد تفضل الخيار الثاني أي التوقيع النصي binary (قابلة للطباعة
إلى 'gpg' لكلاهما نفس القوة)، يمكنك تحويل مخرجات signature
ثم إرسال محتويات ذلك الملف 'output--' أو 'o-' بدلاً من الخرج القياسي بواسطة ('file.asc' ملف (مثل
(وذلك بلصق المخرجات في موقع الويب الخاص بخدمة البريد (المجاني
SMTP. أو تمررها عبر أنبوب إلى برنامج إرسال البريد بواسطة بروتوكول

$ gpg --output file.sig --sign file.txt
$ gpg --output file.asc --clearsign file.txt

الملف الناتج يحتوي الملف الأصلي والتوقيع معاً، عليك تعديله/تحريره لفصل الملف الأصلي يمكن أن تتم
gpg أو أن تطلب من ،clearsign يدوياً في حالة التوقيع النصي
Detached لهذا يفضل بعض الناس ما يسمى بالتوقيع المنفصل .sign القيام بذلك خصوصاً في حالة
حيث يحفظ التوقيع في ملف منفصل، ونرسل الملفين (الوثيقة 'signatures
(والتوقيع) معاً (مثلاً يمكن أن يرسل التوقيع كملف في مرفقات الرسالة

$ gpg --output file.txt.sig --detach-sig file.txt

وأي تعديل في أيهما سوف يفسده "file.txt" لا يصلح إلا كتوقيع للملف "file.txt.sig" الملف الناتج
clear text ASCII-armored ويظهر عند التحقق. إذا كنت تفضل التوقيع النصي
كما يلي 'armor--' أضف الخيار format

$ gpg --output file.txt.asc --armor --detach-sig file.txt

مثلاً، توقع أغلب downloads حالياً ينشر استخدام التواقيع المنفصلة في التحقق من سلامة التنزيل
لأقراصها بهذه الطريقة) حيث تجد ملف ISO images التوزيعات صور
في جميع .md5sum مقابل لكل ملف يمكن تنزيله، هذه الطريقة أفضل من مجرد '.sig' أو '.asc'
الحالات يلزم المفتاح الخاص (السري) لعمل التوقيع لهذا يسألك البرنامج
إذا كان هناك أكثر من مستخدم (أكثر من مفتاح خاص) حدد الذي تريد ،passphrase عن جملة السر
'u-' بواسطة.

متبوعة بملف التوقيع المنفصل 'verify--' إذا حصلت على ملف موقع وتريد فحص التوقيع استعمال الخيار
(إن وجد) ثم الملف الموقع

$ gpg --verify file.txt.sig file.txt

('clearsign--' أو 'sign--' إذا حصلت على الوثيقة والتوقيع معاً في ملف واحد (أو أنه ولّد بواسطة
:لاستخراج الوثيقة الأصلية دون التوقيع 'decrypt--' استعمل

$ gpg --output file.txt --decrypt file.sig

تم بحمد الله تعالى

المصادر والمراجع

هذا الكتيب مفتوح (حر) خاضع لرخصة)

نسخ أو تصوير أو الإقتباس من هذا الكتاب لا يعد مخالفاً للقانون

GNU FDL (أي GNU Free Documentation License

اهم المراجع:وهى

كتاب لينكس الشامل : للأستاذ :مؤيد السعدي

وايضا

The GNU Privacy Handbook

من مؤسسة جنو

لمراسلة المؤلف على البريد الالكتروني

لصاحبة : على عبد الغني

blade.vp2020@gmail.com

تم التنسيق بواسطة : محمد عثمان "مجموعة مستخدمي نظام جنو/لينكس"موقعنا على الفيس

https://www.facebook.com/groups/113775252120817/