PGP Web of Trust: Core Concepts Behind Trusted Communication

By *Rianne Schestowitz*
Created *07/02/2014 - 7:56pm*
Submitted by Rianne Schestowitz on Friday 7th of February 2014 07:56:30 PM Filed under Security [1]

If you've ever used Linux, you've most likely used OpenPGP without even realizing it. The open-source implementation of OpenPGP is called GnuPG (stands for "GNU Privacy Guard"), and nearly all distributions rely on GnuPG for package integrity verification. Next time you run "yum install" or "yum update", each package will be verified against its cryptographic signature before it is allowed to be installed on your system. This assures that the software has not been altered between the time it was cryptographically signed by distribution developers on the master server, and the time it was downloaded to your system.

However, far fewer people have actually used GnuPG for what it was originally designed for -- secure exchange of information in an untrusted medium (such as the internet), and even fewer have a good understanding of how the trust relationships are supposed to work.

In this mini series of articles, we'll take a look at what the web of trust is and how to use it to set up a secure and trusted communication.

Read more [2]

Security

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] http://www.linux.com/learn/tutorials/760909-pgp-web-of-trust-core-concepts/