Using Signed Archives

In this installment of the mini-howto series, we're going to cover signed archives. Not so long ago, a large number of community servers were cracked. Among the large numbers of machines that were cracked were the machines that housed the gnu cvs repositories and Debian's packaging machines. This resulted in a *huge* mess; essentally every line of source code in every program had to be audited one line at a time to make sure the crackers hadn't inserted any sort of malicious code. Clearly, *something* needed to be done so that this could never happen again. The community at large needed a way to detect archive tampering.

And so signed archives were added into Bazaar. With a signed archive, every single patch is signed, via gnupg. That way, if the server that holds an archive is cracked, the source codes integrity can be validationed (in the absence of successfuly preimage attacks on SHA1). If the archive survives a proper signature check, then you know that the archive hasn't been tampered with.

Bazaar requires gnupg be installed to use and create signed archives. If it is not installed, you will need to do so to continue.

If you are interested in signed archives, then it is from one of two contexts; either you want get from someone elses' signed archive, or you want to make a signed archive.

Using someone elses archive

Baz will automatically detect when archives are signed. If the signature cannot be verified, the archive will be treated as altered and a error will be printed to stderr. If you do not have the GPG key for the person whos archive it is on your keyring, the archive won't be accessible. One way to ensure you have the required keys is to set *keyserver-options auto-key-retrieve* in your *.gnupg/gpg.conf*.

The default policy for Bazaar is to require a valid signature from anyone on a revision. You can create a stricter policy by editing *~/.arch-params/archives/$archivename* and setting one or more of:

- *allowed_ids=john@example.com*
- *allowed_ids=E12334458763524*
- *allowed_fingerprints=E12345677627865429642964236266*

Creating your own signed archive

Not written yet,

title: Using Remote Signed Archives

license: General Public License, V2

copyright: (C) 2004, 2005 Canonical Ltd.

authors: James Blackwell <jblack@gnuarch.org>, Robert Collins <robert.collins@canonical.com>