Linux distribution packaging and Bitcoin

July 2013

This note summarises the dangers inherent in the Linux distribution packaging model for Bitcoin, and forms a request from upstream maintainers to not distribute Bitcoin node software as part of distribution package repositories without understanding the special requirements of Bitcoin.

Distributors typically unbundle internal libraries and apply other patches for a variety of generally good reasons, in addition to ensuring that security-critical fixes can be applied once, rather than multiple times for many different packages. In most cases, the common distribution packaging policy has many advantages.

However, Bitcoin nodes are an unusual category of software: they implement a complex group consensus in which every client verifies the behaviour of every other exactly. Even an exceptionally subtle change - including apparently harmless bugfixes - can cause a failure to reach consensus. A consensus failure of one client is a security risk to the user of that client. A significant number of nodes failing to reach consensus - as happened in March 2013 due to a change in database libraries[1] - is a critical problem that threatens the functionality and security of the system for all users.

For this reason, it is vital that as much of the network as possible uses unmodified implementations that have been carefully audited and tested, including dependencies. For instance, if the included copy of LevelDB in bitcoind is replaced by a system-wide shared library, any change to that shared library requires auditing and testing, a requirement generally not met by standard distributor packaging practices.

Because distributed global consensus is a new area of computer science research, the undersigned hereby ask that distributors refrain from packaging Bitcoin node software (including bitcoind and Bitcoin-Qt) and direct users to the upstream-provided binaries instead until they understand the unique testing procedures and other requirements to achieve consensus. Beyond being globally consistent, upstream binaries are produced using a reproducible build system[2], ensuring that they can be audited for backdoors.

Signed,

Gavin Andresen
Mike Hearn
Mark Friedenbach
Luke Dashjr
Peter Todd
Gregory Maxwell

GPG signatures can be found here:
http://luke.dashjr.org/tmp/code/20130723-linux-distribution-packaging-and-bitcoin.md.asc

---

[1] https://en.bitcoin.it/wiki/BIP_0050
[2] http://gitian.org/