Subject: Re: WebUpdater
Posted by mr_ped on Wed, 19 May 2010 10:27:00 GMT
View Forum Message <> Reply to Message

Well, in ideal world some of the things has to pushed a bit farter (although your list is quite exhaustive already):

1) make the downloader modular (HttpClient behind abstract interface), so it can be exchanged with rsync/zsync/bittorrent/... modules later (designing such unified API will be tricky though). Also some modules may support user authentication, so you can make sure your update server does service only registered users.

2) there's no security incorporated, I think this is under "industrial standard" (or better to say the industrial standard is too low, as I'm looking around at some industry solutions around me). There are several levels where checking is desirable:
- download integrity (md5 sums as you proposed)
- user is authorized to upgrade to desired version (A)
- parent server verification (B)
- encrypted communication with server (C)

A) things to consider
- local user's installation vs global one
- corporate permissions, like allowing/forcing certain versions per user, etc. (implementation shouldn't be part of this updater, but there should be interface/hooks for this?)

B) you have to verify the update server is the real one. I think the digital signing of final update files is a must, eventually signed revision files with versions+md5sums would be good to discover problems before file downloading.

Also md5sum as is is already too weak, I would used at least sha1+md5 or sha2 class (+md5 doesn't hurt).

C) the https or other encrypted downloader would be nice, although that can be worked around by using 7z with password and sending only zip files between app and server, so there are no public data for somebody eavesdropping. (but https would be more robust, as the encrypted zip files are useless once the password leaks .. still better than nothing)

hmm.. this should help to cover both open applications (where only the integrity is a concern) and closed applications where you want to have server on internet, but you don't want to give away any info to guests, only to your registered customers (plus you still need the integrity checks anyway).