Ruby - Bug #18356

Please replace use of unsafe MD5 with another digest algorithm

11/22/2021 11:39 AM - pvalena (Pavel Valena)

Status:	Third Party's Issue		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:		**Backport:**	2.6: UNKNOWN, 2.7: UNKNOWN, 3.0: UNKNOWN

Description

Similarly to https://bugs.ruby-lang.org/issues/18272

Context

When working on a new version of RHEL (with Ruby 3.0), the requirement is to have a better security (remove unsafe digests or limit the use for non-security purposes). This would be achieved with using OpenSSL 3.0 as well, which will have a raised security level by default, forbidding the use of unsafe digests.

Issue

MD5 does not conform to the security requirements, and its replacement would be preferred.
Currently, the following files indicate it's use:

```
rubygems/package.rb:    return super unless gem.start.include? 'MD5SUM ='
bundler/compact_index_client/cache.rb:          name += "-#{SharedHelpers.digest(:MD5).hexdigest(name).downcase}"
bundler/compact_index_client/updater.rb:          SharedHelpers.digest(:MD5).hexdigest(File.read(path))
bundler/source/rubygems/remote.rb:            uri_digest = SharedHelpers.digest(:MD5).hexdigest(uri_parts.compact.join("."))
bundler/vendor/thor/lib/thor/runner.rb:      :filename   => Digest::MD5.hexdigest(name + as),
```

Alternative solution

The use for non-security purposes might be indicated with setting an internal variable (when using OpenSSL implementation), which would allow the use of MD5 (although forbidden via OpenSSL setting). Do you think this would be possible?

Question

AFAICT in Ruby it is used for non-security purposes only. Could you confirm that?

Additional information

The tests failed on digests/md5 removal:
https://gist.github.com/pvalena/ce6af993c6fe7c825cc41be81e1944ad

Related issues:

Related to Ruby - Feature #18272: Please replace unsafe SHA1 with another dig...	**Third Party's Issue**

History

#1 - 11/22/2021 11:48 AM - nobu (Nobuyoshi Nakada)

- Related to Feature #18272: Please replace unsafe SHA1 with another digest algorithm added

#2 - 11/22/2021 04:19 PM - byroot (Jean Boussier)

This is all from bundler / rubygems, so I believe we should close as a third party issue.

#3 - 11/22/2021 05:23 PM - pvalena (Pavel Valena)

byroot (Jean Boussier) wrote in #note-2:

> This is all from bundler / rubygems, so I believe we should close as a third party issue.

Please note that was a filtered list, there are other dependecies, such as pop3/imap, cgi, and other net/ uses.

On the tests side - a test is failing on

```
/builddir/build/BUILD/ruby-3.0.2/test/net/http/test_buffered_io.rb: cannot load such file -- digest/md5
```

(There might be more issues as well, I'm still investigating.)

Also, there's md5 implementation in ext/digest/md5/. Could the tests be adjusted not to fail on md5 absence?

#4 - 11/22/2021 06:07 PM - jeremyevans0 (Jeremy Evans)

pvalena (Pavel Valena) wrote in #note-3:

> byroot (Jean Boussier) wrote in #note-2:
>
> > This is all from bundler / rubygems, so I believe we should close as a third party issue.
>
> Please note that was a filtered list, there are other dependecies, such as pop3/imap, cgi, and other net/ uses.

Can you please provide an unfiltered list, and for each case where it is currently used, an analysis of the effects of removing MD5 and replacing it with something else, including how backwards compatibility will be handled? Each case will need to be considered separately.

> On the tests side - a test is failing on
>
> ```
> /builddir/build/BUILD/ruby-3.0.2/test/net/http/test_buffered_io.rb: cannot load such file -- digest/md5
> ```
>
> (There might be more issues as well, I'm still investigating.)
>
> Also, there's md5 implementation in ext/digest/md5/. Could the tests be adjusted not to fail on md5 absence?

Just like SHA1, I think we are against removal of MD5, since there are valid uses that are still considered secure (such as use of HMAC-MD5). So I don't think it is wise to modify the tests to handle the absence of MD5. As indicated above, we can certainly consider switching internal uses of MD5/SHA1 to something better, but that needs to be handled on a case-by-case basis.

#5 - 11/24/2021 12:28 AM - hsbt (Hiroshi SHIBATA)

- Status changed from Open to Third Party's Issue

Please file them to https://github.com/rubygems/rubygems/issues.

#6 - 11/24/2021 09:06 AM - byroot (Jean Boussier)

> Please note that was a filtered list, there are other dependecies, such as pop3/imap, cgi, and other net/ uses.

All theses are "bundled gems", they're basically vendored in ruby but have their own issue trackers e.g. https://github.com/ruby/net-pop

I greped myself for Digest::MD5 in the actual stdlib, and all I could find is cgi/session where the session ID is hashed with MD5 to create a file path, so not a crypto use and changing it would break backward compatibility.

So I'm of the opinion that this issue is not actionable from a Ruby standpoint and should be closed.