

0. git checkout

```
# Audit of 04af5c7cbff47b17bd4b0153330028adb28eae4c
git checkout -b audit-pyeron-04af5c7 04af5c7cbff47b17bd4b0153330028adb28eae4c
```

1. git diff

```
# review all changes since e8529e95d89d3f519a31ef7de5bd7f0d0d318e8c
git diff e8529e95d89d3f519a31ef7de5bd7f0d0d318e8c | grep ^diff | sed -e 's/ b\./.*$/; s/diff --git a\\/'
```

1.1. Added Files

```
1.1.1. doc/trust/audits/p/y/pyeron,jason/audit-report-2014-12-09-e8529e95d89d3f519a31ef7de5bd7f0d0d318e8c.pdf
1.1.2. rebranding_notes
```

1.2. Changed Files

```
1.2.1. src/Common/Apidrvr.h
1.2.2. src/Common/BootEncryption.cpp
1.2.3. src/Common/BootEncryption.h
1.2.4. src/Common/CipherShed.ico
1.2.5. src/Common/CipherShed_Volume.ico
1.2.6. src/Common/CipherShed_mounted.ico
1.2.7. src/Common/Common.h
1.2.8. src/Common/Dlgcode.c
1.2.9. src/Common/Dlgcode.h
1.2.10. src/Common/Language.xml
1.2.11. src/Common/SecurityToken.h
1.2.12. src/Common/Tcdefs.h
1.2.13. src/Common/Textual_logo_288dpi.bmp
1.2.14. src/Common/Textual_logo_96dpi.bmp
1.2.15. src/Common/Volumes.c
1.2.16. src/Common/Xml.c
1.2.17. src/Driver/BuildDriver.cmd
1.2.18. src/Driver/DriveFilter.c
1.2.19. src/Driver/DriveFilter.h
1.2.20. src/Driver/Driver.rc
1.2.21. src/Driver/Driver.vcproj
1.2.22. src/Driver/Ntdriver.c
1.2.23. src/Driver/Sources
1.2.24. src/Format/CipherShed_Wizard.bmp
1.2.25. src/Format/Format.rc
1.2.26. src/Format/Format.vcproj
1.2.27. src/Format/InPlace.c
1.2.28. src/Format/Tcformat.c
1.2.29. src/Main/Xml.cpp
1.2.30. src/Makefile
1.2.31. src/Mount/Drive_icon_96dpi.bmp
1.2.32. src/Mount/Drive_icon_mask_96dpi.bmp
1.2.33. src/Mount/Logo_288dpi.bmp
1.2.34. src/Mount/Logo_96dpi.bmp
1.2.35. src/Mount/Mount.c
1.2.36. src/Mount/Mount.rc
1.2.37. src/Mount/Mount.vcproj
1.2.38. src/Mount/System_drive_icon_96dpi.bmp
1.2.39. src/Mount/System_drive_icon_mask_96dpi.bmp
1.2.40. src/Setup/CipherShed_setup.bmp
1.2.41. src/Setup/ComSetup.cpp
1.2.42. src/Setup/ComSetup.rgs
1.2.43. src/Setup/Setup.c
1.2.44. src/Setup/Setup.h
1.2.45. src/Setup/Setup.ico
1.2.46. src/Setup/Setup.rc
1.2.47. src/Setup/Setup.vcproj
1.2.48. src/Setup/Wizard.c
1.2.49. src/Volume/Volume.cpp
1.2.50. src/Volume/VolumeHeader.cpp
```

2. Changes

2.1. Documentation

- 2.1.1. Audit report (#1.1.1).
- 2.1.2. Developer notes on CipherShed installation & upgrade from TrueCrypt (1.1.2).
- 2.1.3. Update on copyright statements in file 1.2.8.
- 2.1.4. Added developer documentation in files 1.2.8, 1.2.9, 1.2.15, 1.2.18, 1.2.19, 1.2.22, 1.2.27, 1.2.28, 1.2.41, 1.2.43, 1.2.48, 1.2.49 & 1.2.50.
- 2.1.5. Update the application version numbers in the files 1.2.12, 1.2.20, 1.2.25, 1.2.36, 1.2.46.

2.2. License Compliance

2.2.1. Undo rename TrueCrypt to CipherShed

- 2.2.1.1. Some uses of "TrueCrypt" are functional in nature; as such changes will prevent proper operation. It is important to ensure these are not branding, but functional.
- 2.2.1.2. Developer observations are recorded in [1.1.2].
- 2.2.1.3. The following files are modified to revert the changes to the functional uses of the "TrueCrypt" string 1.2.2, 1.2.3, 1.2.8, 1.2.9, 1.2.10, 1.2.16, 1.2.17, 1.2.20, 1.2.21, 1.2.22, 1.2.23, 1.2.25, 1.2.29, 1.2.35, 1.2.43, 1.2.44 & 1.2.49.

2.2.2. Change images & logos

- 2.2.2.1. The icon files 1.2.4, 1.2.5, 1.2.6 & 1.2.45 were redacted to simple paint brush alternatives. The files open without error in visual studio 2008 and TortoiseGitDiff. There is no unexpected data in the files.
- 2.2.2.2. The bitmap files 1.2.13, 1.2.14, 1.2.24, 1.2.31, 1.2.32, 1.2.33, 1.2.34, 1.2.38, 1.2.39, & 1.2.40 were redacted to simple paint brush alternatives. The files open in TortoiseGitDiff and Adobe Photoshop without error. There is no unexpected data in the files.

2.3. Updates in functionality

2.3.1. New operating system support

- 2.3.1.1. Added support for Windows 8+ in files 1.2.7, 1.2.8, 1.2.10 & 1.2.22.

2.3.2. TrueCrypt upgrade support

- 2.3.2.1. Update the windows registry changing sub key names, like is described in <http://msdn.microsoft.com/en-us/library/k32htkctc.aspx> in file 1.2.42
- 2.3.2.2. Detection of old TrueCrypt installed during upgrade in file 1.2.43 and the corresponding header file 1.2.44.
- 2.3.2.2.1. Created an uninstaller function, DoTrueCryptFilesUninstall, for the old TrueCrypt files. It is called from DoInstall on migration upgrades.
- 2.3.2.2.2. Created an uninstaller function, DoTrueCryptShortcutsUninstall, for the old TrueCrypt shortcuts. It is called from DoInstall on migration upgrades
- 2.3.2.2.3. Introduced the 'bCipherShedMigration' status and concept when the old version is less than 0x0730.
- 2.3.2.2.4. Moved the trailing slash on installation path correction code prior to installation type conditional logic since 'szDir' is used in the CipherShed registry migration.
- 2.3.2.2.5. Added windows registry keys ('MigrationPath', etc.) to facilitate upgrade handling.
- 2.3.2.2.6. Additional logic for handling hidden encrypted OS
- 2.3.2.3. In file 1.2.48 checks are made for the legacy files and configuration
- 2.3.2.3.1. It checks if the files on disk exist and are modifiable.
- 2.3.2.3.2. It checks for the existence of Registry keys
- 2.3.2.3.3. It specifically prompts the user to choose between TrueCrypt and CipherShed.

2.3.3. Other Installation Enhancements

- 2.3.3.1. Notify "Shell" on link / shortcut changes in file 1.2.43, using SHChangeNotify.
- 2.3.3.2. On error, closes the COM library on the apartment, releases any class factories, other COM objects, or servers held by the apartment, disables RPC on the apartment, and frees any resources the apartment maintains in file 1.2.43.
- 2.3.3.3. Allows a user to force continue the execution without the required Administrative privileges in file 1.2.43.

2.4. Updates to the build

2.4.1. PKCS

- 2.4.1.1. The include path for the PKCS headers is updated in the files 1.2.11, 1.2.26, 1.2.30, 1.2.37 & 1.2.47.

2.5. Other changes

- 2.5.1. Changed the case of 'CipherShed_Wizard.bmp' in 1.2.25, 1.2.26.

3. Provenance

3.1. Commits

3.1.1. HEAD commit

The 04af5c7cbff47b17bd4b0153330028adb28eae4c is a signed merge of a previous audit branch signed commit 55e040f and the signed commit d79fb95. Both branches have a common parent commit e8529e9, and that commit is subject to a previous audit.

3.1.2. Commit graph

```
*      04af5c7cbff47b17bd4b0153330028adb28eae4c
|\
| * 55e040fcdc24672cf043f1a0d06d82314792e6a6
| * b52fb1f306d2533a9e93296b8c99dfb2e1b4a5aa
* | d79fb95128a8bd46e66d05fd8e540b474bc634f0
* | 1cf2381a0974f1031f349d23e9f755d774f7fe09
* | 2d239672f23d85490d74142ec1440cfc9b017f42
* | 967fd845c1c185f4c66ed74b8ea56a50216bcf5b
* | 97c20680757bfb56a076ea60648e1644b0e44648
* | bcd72912677b5070947c06116bce908187188264
* | a1434d2f03225400908f52fade2ef1f152e4352d
* | c94f3741e5da99f19311635b0389741c83ab4581
* | d2e84e66f65002fc46e25b75a72fcc0760990cdd
* | bee06736083eaf825c81bfd647d6d76b57f34d3e
* | 90c948cb3f63fc7348f4124e4ac6acfc3d9e7257f
* | 72b757635f3e37b21ad98f1801459cf46e6f9960
* | 3ab260c5b8a05f38be763be28dc75eaf4a71fdbe
* | 6b669618c1deb5528c4b02d7dd08b8f9aaeefe5f
* | 230b60f143158489455810af918e978819f6179a
* | f014d9995c0ea4c6617ee83687d5883d54258f4b
* | be65309388a8865a59ee9b399bd2fd882904b983
* | 0blc3f689b8567dcf1bde1dd9c01f6f18afe262a
* | 6b59524f8c16c3940a84839f82a9ddfb834f36a6
* | e6306568592bc120f8fe37cf190f7d5acd487e6d
* | f843ce1e706724ef072ce2ee74b6bd73c4655e8a
* | 905d875b32794846531fe208397f674d4dfa9cb5
* | 9ee0976a1e235ed1bdfd826db8bcf56e40638481
* | bef5be1788f838350d33a7102d55a62a38e8a605
* | 701968d0f4ad7cc57bea744e0916115b7903713b
* | 42bcef7a9d4bfd9614579bc74bc8652a0b7a4a9f
* | 345f69e3e619f26efcb0c03c0c89048aa818ac6c
* | e3113d69274ab40353b09e13527738057169e0ba
* | 62237751f5d4c123fd46981ebc3700337a6179d8
* | bb7708fe04b62ddbce4dfalf0c521834627b085a
* | 98f8d86a9688f161a83ca0d67f2c704babc8f292
* | bd6d919b1731de1a4563603fa513blac13edab3a
* | ba21e78e6acc08ad70f05e5b2971cf752d8e6cbf
* | 5fd8c21f6880fd9f693fcf26be0f852c04a3d85c
* | 841417e97de7dc564999e328513d3bb9c7a96bcf
* | d9772543d40fea7e8be643647b9f68d00c599318
* | a045a437183ebc1d7ab826f4c1a8cb7b23d19355
* | 878007e7c6497f376da88046968e1ee96ea00ba4
* | d5b74c8541748786eb151d67a5224c2ba224d1dd
* | 207cf31434c77d2795376c9d857358f10938a844
* | b0cee7bb8501c7355376c058b116a097b9bcfe4b
* | 0a8919173eb7589d366c92a2302592b218f2dd89
* | a400b2d4913b264ed242f5c8b1750ff587d8e66d
* | 8fa6489c256d8fd4c9a5331e443c1b8f90f25017
* | f0b8fad71493a25835cb252760b22d0dfd3219ee
* | 47f6e138450781fed82a11f28b0586988b4d8f11
* | b7767a574afda431f34fdb31026f6a56130799ed
* | 34f618feb0d97765e87a5b038295fbae8316a0c2
* | 27498d0bc0c88854b87ce0d80922bd5c052248a8
* | f66f5d93ff25a1cdbc2ac5537f361621d2b15f4
* | 4d5b52d440d3a64953a6d7ef3cbb81c8d289e392
* | a0edd584fc314434b79da764104310a69eae9b08
* | 1be891a0f7dfa947178250939dcf4cee596c32a1
* | ad373308546493adb32cc80208c4b286e532880f
* | 2c5e5d1f660b0970f929540c906a7ab02d310e30
* | d0dc8ce0e49a94f0ea23dc531e2ec462c1ea9ab3
* | e91a2fd4ce51b9989709389099377b8050c9f447
* | 9b3178aeb53fbadd99ad19a9d68d7745e28b7b61
* | 3641f4c589feb0f13a8a0f806dc21543597f2528
* | 783b98ebb0c75aabf0a47c6131e2c678c503cd90
* | c763793c0ecf63a05f23f050e05af1180dfe54d5
* | be25f751df34847563f2ffa98abf7b142b5d5b1
* | 8d8091fe6ca57271c8ef1cee4383bf32fd27b2a2
* | 908653612c1a7e876a944c537a8bdb4523032ae0
* | c56518137d026bec47a7ed8bb9f5cd827686c0da
* | b8bf898331164eala89a63699ad375aee04633e0
* | 07fb47ef814bf3ae6b518422236163a97a836904
|/
* e8529e95d89d3f519a31ef7de5bd7f0d0d318e8c
```

3.1.3. Selected critical commits' log entries

3.1.3.1. commit 04af5c7cbff47b17bd4b0153330028adb28eae4c
gpg: Signature made Tue, Dec 09, 2014 14:21:19 EST using RSA key ID DA0848AD
gpg: Good signature from "Jason Pyeron <jpyeron@pdinc.us>"
Merge: d79fb95 55e040f
Author: Jason Pyeron <jpyeron@pdinc.us>
Date: Tue Dec 9 14:20:53 2014 -0500

import last audit: audit-pyeron-d79fb95

3.1.3.2. commit b52fb1f306d2533a9e93296b8c99dfb2e1b4a5aa
gpg: Signature made Tue, Dec 09, 2014 14:18:08 EST using RSA key ID DA0848AD
gpg: Good signature from "Jason Pyeron <jpyeron@pdinc.us>"
Author: Jason Pyeron <jpyeron@pdinc.us>
Date: Tue Dec 9 14:17:52 2014 -0500

audit of e8529e95d89d3f519a31ef7de5bd7f0d0d318e8c

3.1.3.3. commit d79fb95128a8bd46e66d05fd8e540b474bc634f0
gpg: Signature made Thu, Oct 09, 2014 17:10:59 EDT using RSA key ID 32DA3E69
gpg: Good signature from "Rocki H. (CipherShed) <rocki.hack@gmail.com>"
Primary key fingerprint: A2D4 8761 ED9F 749C B7A3 7CEE 6AC4 8E39 32DA 3E69
Author: rockihack <rocki.hack@gmail.com>
Date: Thu Oct 9 22:49:02 2014 +0200

Added Hiberboot warning.

3.1.3.4. commit e3113d69274ab40353b09e13527738057169e0ba
gpg: Signature made Mon, Aug 11, 2014 12:38:09 EDT using RSA key ID 32DA3E69
gpg: Good signature from "Rocki H. (CipherShed) <rocki.hack@gmail.com>"
Primary key fingerprint: A2D4 8761 ED9F 749C B7A3 7CEE 6AC4 8E39 32DA 3E69
Author: rockihack <rocki.hack@gmail.com>
Date: Mon Aug 11 18:38:09 2014 +0200

Changed version number to 0.73 (0x0730).

3.1.3.5. commit 62237751f5d4c123fd46981ebc3700337a6179d8
Author: rockihack <rocki.hack@gmail.com>
Date: Mon Aug 11 18:27:46 2014 +0200

Added legacy IsFileInUse check.

3.1.3.6. commit 841417e97de7dc564999e328513d3bb9c7a96bcf
gpg: Signature made Sun, Aug 10, 2014 16:10:08 EDT using RSA key ID 32DA3E69
gpg: Good signature from "Rocki H. (CipherShed) <rocki.hack@gmail.com>"
Primary key fingerprint: A2D4 8761 ED9F 749C B7A3 7CEE 6AC4 8E39 32DA 3E69
Author: rockihack <rocki.hack@gmail.com>
Date: Sun Aug 10 22:10:08 2014 +0200

Fix: Reverted several places in Setup.c

3.1.3.7. commit d9772543d40fea7e8be643647b9f68d00c599318
Author: rockihack <rocki.hack@gmail.com>
Date: Sun Aug 10 21:56:17 2014 +0200

Fix: Reverted driver names in Setup.h

3.1.3.8. commit 4d5b52d440d3a64953a6d7ef3cbb81c8d289e392
gpg: Signature made Fri, Aug 08, 2014 10:34:53 EDT using RSA key ID 32DA3E69
gpg: Good signature from "Rocki H. (CipherShed) <rocki.hack@gmail.com>"
Primary key fingerprint: A2D4 8761 ED9F 749C B7A3 7CEE 6AC4 8E39 32DA 3E69
Author: rockihack <rocki.hack@gmail.com>
Date: Tue Aug 5 00:11:50 2014 +0200

Added comments to DoServiceUninstall.

3.1.3.9. commit a0edd584fc314434b79da764104310a69eae9b08
Author: rockihack <rocki.hack@gmail.com>
Date: Mon Aug 4 23:20:38 2014 +0200

Added comments to DoDriverUnload.

3.1.3.10. commit 1be891a0f7dfa947178250939dcf4cee596c32a1
Author: rockihack <rocki.hack@gmail.com>
Date: Mon Aug 4 17:21:05 2014 +0200

Added comments to DoUninstall.

3.1.3.11. commit ad373308546493adb32cc80208c4b286e532880f
Author: rockihack <rocki.hack@gmail.com>
Date: Mon Aug 4 16:36:04 2014 +0200

Added comments to SetInstallationPath.

3.1.3.12. commit 2c5e5d1f660b0970f929540c906a7ab02d310e30
Author: rockihack <rocki.hack@gmail.com>
Date: Mon Aug 4 16:28:06 2014 +0200

Added comments to UninstallDlgProc.

3.1.3.13. commit d0dc8ce0e49a94f0ea23dc531e2ec462clea9ab3
Author: rockihack <rocki.hack@gmail.com>
Date: Sun Aug 3 14:28:09 2014 +0200

Added comments on DoInstall.

3.1.3.14. commit e91a2fd4ce51b9989709389099377b8050c9f447
Author: rockihack <rocki.hack@gmail.com>
Date: Sun Aug 3 13:49:46 2014 +0200

Added comments to SetSystemRestorePoint.

3.1.3.15. commit 9b3178aeb53fbadd99ad19a9d68d7745e28b7b61
Author: rockihack <rocki.hack@gmail.com>
Date: Sun Aug 3 13:28:05 2014 +0200

Added comments to UpgradeBootLoader.

3.1.3.16. commit 3641f4c589feb0f13a8a0f806dc21543597f2528
Author: rockihack <rocki.hack@gmail.com>
Date: Sun Aug 3 13:01:50 2014 +0200

Changed the 'Storage Volumes' comment to make it clearer.

3.1.3.17. commit 783b98ebb0c75aabf0a47c6131e2c678c503cd90
Author: rockihack <rocki.hack@gmail.com>
Date: Wed Jul 30 19:27:29 2014 +0200

Added comments to DetermineUpgradeDowngradeStatus.

3.1.3.18. commit c763793c0ecf63a05f23f050e05af1180dfe54d5
Author: rockihack <rocki.hack@gmail.com>
Date: Wed Jul 30 18:05:13 2014 +0200

Added comments to setup WinMain.

3.1.3.19. commit be25f7551df34847563f2ffa98abf7b142b5d5b1
Author: rockihack <rocki.hack@gmail.com>
Date: Sun Jul 27 18:27:33 2014 +0200

Fixed pkcs11.h include path (we don't need PKCS11_INC anymore).

3.1.3.20. commit 8d8091fe6ca57271c8ef1cee4383bf32fd27b2a2
Author: rockihack <rocki.hack@gmail.com>
Date: Sun Jul 27 14:52:36 2014 +0200

Try to load TrueCrypts driver if CipherSheds driver does not exist.

3.1.3.21. commit 908653612c1a7e876a944c537a8bdb4523032ae0
Author: rockihack <rocki.hack@gmail.com>
Date: Sun Jul 27 14:51:06 2014 +0200

Added WIN32_ROOT_PREFIX_LEGACY constant.

3.1.3.22. commit c56518137d026bec47a7ed8bb9f5cd827686c0da
Author: rockihack <rocki.hack@gmail.com>
Date: Sat Jul 26 22:38:54 2014 +0200

Added comments on Apidrvr.h constants.

3.1.3.23. commit b8bf898331164eala89a63699ad375aee04633e0
Author: rockihack <rocki.hack@gmail.com>
Date: Sat Jul 26 22:06:35 2014 +0200

Reverted mutex names to be compatible with TrueCrypt.

3.1.3.24. commit 07fb47ef814bf3ae6b518422236163a97a836904
Author: rockihack <rocki.hack@gmail.com>
Date: Sat Jul 26 15:10:43 2014 +0200

Added comment on Storage Volumes class guid.

3.1.3.25. commit e8529e95d89d3f519a31ef7de5bd7f0d0d318e8c
Merge: 6bccfd6 344df5d
Author: Stephen R Guglielmo <srg@guglielmo.us>
Date: Tue Jul 1 12:11:39 2014 -0400

Merge pull request #15 from srguglielmo/master

Update README with new links

3.2. Commit analysis

The merge commit [3.1.3.1] is signed. This commit is the merge of a previous audit branch and a sequence of developer commits.

The audit branch contains only signed commits since commit [3.1.3.25], the base commit of this audit and the subject of the last audit [7.1.1]. It is further noted that the audit branch does not modify any files outside of the audit folder.

The developer commits are terminated with a signed commit [3.1.3.3]. This branch is a sequence of commits by two authors [3.2.1.1] & [3.2.1.3]. The each commit in the sequence is signed up to and including commit [3.1.3.4], whose unsigned parent is commit [3.1.3.5]. Both commits [3.1.3.4] & [3.1.3.5] are made by the same author.

The developer branch commit sequence continues with signed commits up to an including commit [3.1.3.6], whose unsigned parent is commit [3.1.3.7]. Both commits [3.1.3.6] & [3.1.3.7] are made by the same author.

The developer branch commit sequence continues with signed commits up to an including commit [3.1.3.8], whose unsigned parent is commit [3.1.3.9]. The commits [3.1.3.9], [3.1.3.10], [3.1.3.11], [3.1.3.12], [3.1.3.13], [3.1.3.14], [3.1.3.15], [3.1.3.16], [3.1.3.17], [3.1.3.18], [3.1.3.19], [3.1.3.20], [3.1.3.21], [3.1.3.22], [3.1.3.23] and [3.1.3.24] are not signed but a sequence by a single author. The sequence is ended by a signed commit by the same author in commit [3.1.3.8].

The commit [3.1.3.25] is the subject of an audit [7.1.1] and is not signed. Commit [3.1.3.25] has a signed parent commit [3.1.3.2].

3.2.1. Authors

3.2.1.1. Mr. Cox - 27498d0bc0c88854b87ce0d80922bd5c052248a8
3.2.1.2. Mr. Guglielmo - e8529e95d89d3f519a31ef7de5bd7f0d0d318e8c
3.2.1.3. Mr. Hack - 07fb47ef814bf3ae6b518422236163a97a836904
3.2.1.4. Mr. Pyeron - b52fb1f306d2533a9e93296b8c99dfb2e1b4a5aa

3.2.2. Status

Given the woven signed and unsigned commits of more than two well known participants it is clear that the source's history can be trusted as valid. The SCM system provides cryptographic validation as to the accuracy of the changes made, but not the authorship of a given unsigned commit. The status of this audit is based on the information included in the previous audit included in commit [3.1.3.2].

4. Risks Identified

4.1. Buffer Overflow: sprintf

4.1.1. CAT II - File 1.2.43

- 4.1.1.1. The code in this file executes with elevate permissions.
- 4.1.1.2. The DoTrueCryptShortcutsUninstall function uses szTmp2 string to hold computed paths. The input to sprintf are strings which can be longer than the destination, e.g. 'sprintf (szTmp2, "%s%s", szLinkDir, "\\TrueCrypt.lnk)'.- 4.1.1.3. If the application does not crash from the execution of the sprintf, the modified memory is then passed into system calls, e.g. 'StatDeleteFile (szTmp2)'.

4.2. Buffer Overflow: strcat

4.2.1. CAT II - File 1.2.43

- 4.2.1.1. The code in this file executes with elevate permissions.
- 4.2.1.2. In several locations a path is checked for a trailing backslash (0x5c), and if none is found one is appended. The appending operation never checks if the destination has sufficient allocated memory for one more char.
- 4.2.1.3. Other places the function is used to append arbitrary string constants to a string on the heap, e.g. 'strcat (path, "\\TrueCrypt)".- 4.2.1.4. If the application does not crash from the execution of the strcat, the modified memory is then passed into system calls, e.g. '_stat (path, &st)'.

4.3. Buffer Overflow: strcpy

4.3.1. CAT II - File 1.2.48

- 4.3.1.1. The code in this file executes with elevate permissions as it is called from Setup.c.
- 4.3.1.2. e.g. 'strcpy (WizardDestInstallPath + str_len - suffix_len, "\\CipherShed\\)".

5. Conflict of Interest

5.1. Organizational Conflict of Interest

At this time, I have no organizational conflicts of interest. I am an employee of PD Inc and a member of the CipherShed PMC.

5.2. Developer Conflict of Interest

- 5.2.1. 04af5c7cbff47b17bd4b0153330028adb28eae4c - import last audit: audit-pyeron-d79fb95
- 5.2.2. 55e040fcdc24672cf043f1a0d06d82314792e6a6 - removed word format
- 5.2.3. b52fb1f306d2533a9e93296b8c99dfb2e1b4a5aa - audit of e8529e95d89d3f519a31ef7de5bd7f0d0d318e8c

6. Conclusion

While some of the content being verified was produced by me, the properties of the SCM system along with the analysis presented above should be sufficient for a disinterested 3rd party to validate this audit treating my contributions with the highest skepticism.

This audit did attempt to build the software on Windows, but not on any other platform. The testing was limited to build testing and did not perform any functional validation on the generated binaries. The change set covered by this audit attempts to address the automated changes for license compliance discussed in [7.1.1], and the installation may work for upgrades.

The changes are in 5 clear categories documentation, license compliance, new features, build process and miscellaneous changes.

The documentation [2.1] changes have gone a long way to increase the quality of the software development process.

The license compliance [2.2] changes seem to follow the FSF legal advice describing that a functional item is not copyrighted or trademarked. In specific file system identifiers, registry paths and other critical values are functional and are not intellectual property.

The changes in the build process [2.4] and case correction [2.5] on a file name are natural corrections for a better build.

The new features [2.3] include support for newer operating systems, upgrades from TrueCrypt and installation enhancements. Some of the changes made to support the TrueCrypt upgrade [2.3.2] process introduced potential risks into the installer source code. These risks [4] do not affect the CipherShed installed program or driver.

There was 1 type of risk identified, caused by the use of 3 different functions, it is a Buffer Overflow risk. These risks are noted (see: [7.1.2], [7.1.3] & [7.1.4]) in the project issue and defect tracker. The buffers which are at risk are passed to system calls in the elevated privileged installation application. The risks are determined to be CAT II vulnerabilities and need to be fixed.

It is the conclusion of this audit that the source code has newly introduced risks since the last audit on commit e8529e9 (see: 3.1.3.25 & 7.1.1) and must not be approved as a release or used on production systems.

Jason Pyeron
Principal Consultant
PD Inc
10 W 24th St #100
Baltimore, MD 21218
USA

7. Appendix

7.1. References

- 7.1.1. Audit on e8529e9: <https://github.com/pdinc-oss/CipherShed/blob/audit-pyeron-e8529e9/doc/trust/audits/p/y/pyeron,jason/audit-report-2014-12-09-e8529e95d89d3f519a31ef7de5bd7f0d0d318e8c.pdf>
- 7.1.2. <https://issues.ciphershed.org/issues/27>
- 7.1.3. <https://issues.ciphershed.org/issues/28>
- 7.1.4. <https://issues.ciphershed.org/issues/29>

7.2. Colophon

- 7.2.1. git version 2.1.1 was used on Cygwin.
- 7.2.2. TortoiseGit & TortoiseGitDiff v1.8.9.0 was used on 64bit Windows.
- 7.2.3. Microsoft Word 2003 and Adobe Acrobat 8 Professional were used to produce this report.
- 7.2.4. The commit tree was created by: `git log --pretty=format:"%H" --graph`
- 7.2.5. The developer conflict of interest was created by:

```
git log --pretty=format:"%H%x09%ae%x09%ce%x09%s" |\ngrep jpyeron@pdinc.us |\nsed 's/\t[-a-z@\.]\+\t[-a-z@\.]\+\t/ - /'
```

- 7.2.6. Finding a unique set of authors/committers:

```
cat /tmp/commits.txt |\nwhile read line; \ndo git log -1 --pretty=format:"%H%x09%ae%x09%ce%x0a" $line; \ndone |\nsed 's/^[0-9a-f]\+\t\(.*)\t\(.*)\n2/' |\nsort -u
```

7.3. Commit Index

04af5c7	1, 2, 3, 4, 7	9b3178a	3, 5
07fb47e	3, 6	9ee0976	3
0a89191	3	a045a43	3
0blc3f6	3	a0edd58	3, 4
1be891a	3, 4	a1434d2	3
1cf2381	3	a400b2d	3
207cf31	3	ad37330	3, 5
230b60f	3	b0cee7b	3
27498d0	3, 6	b52fb1f	3, 4, 6, 7
2c5e5d1	3, 5	b7767a5	3
2d23967	3	b8bf898	3, 5
345f69e	3	ba21e78	3
34f618f	3	bb7708f	3
3641f4c	3, 5	bcd7291	3
3ab260c	3	bd6d919	3
42bcef7	3	be25f75	3, 5
47f6e13	3	be65309	3
4d5b52d	3, 4	bee0673	3
55e040f	2, 3, 4, 7	bef5be1	3
5fd8c21	3	c565181	3, 5
6223775	3, 4	c763793	3, 5
6b59524	3	c94f374	3
6b66961	3	d0dc8ce	3, 5
701968d	3	d2e84e6	3
72b7576	3	d5b74c8	3
783b98e	3, 5	d79fb95	2, 3, 4, 7
841417e	3, 4	d977254	3, 4
878007e	3	e3113d6	3, 4
8d8091f	3, 5	e630656	3
8fa6489	3	e8529e9	1, 2, 3, 4, 6, 7, 8, 9
905d875	3	e91a2fd	3, 5
9086536	3, 5	f014d99	3
90c948c	3	f0b8fad	3
967fd84	3	f66f5d9	3
97c2068	3	f843ce1	3
98f8d86	3		