



BOSCH

Invented for life


Safe software delivery

Date: 2018-11-30

Contents

1	Document information	3
1.1	Version history.....	3
2	Software delivery	4
2.1	Risks	4
2.2	Solution.....	4
	Checksum and Hashes	4
3	Verifying the download	6

1 Document information

Project	Bosch Building Technologies software
Version	14
Last modified	 30 November 2018

1.1 Version history

Version	Date	Author	Comment
14	2018-11-30		PAS5
13	2018-11-05		PAS4

2 Software delivery

Bosch software is distributed via the Bosch website, but can also be re-distributed by Bosch partners. It is important for the system-installer to check if the installation file he or she has received, matches exactly with the output of the engineering process. There are several risks that, in the distribution path, changes are made to the installation file. Keyloggers or other spyware could be added to the installation, or in theory video surveillance footage could be routed to external resources.

2.1 Risks

The digital distribution path of the software installation file looks as follows:

1. Installation (zip) file is generated as output of the engineering process.
 - a. The sources are fully protected and there is little risk of modifications of the installation file in this phase.
2. Installation file is uploaded to the Bosch Security Systems website.
 - a. The installation file is distributed within Bosch Security Systems without external exposure. There is little risk of modification of the installation file in this phase.
3. The installation file is downloaded from the Bosch Security Systems website to a "distributor".
 - a. The installation file is distributed over the internet. Due to the point-to-point connection there is little to medium risk of modification of the installation file in this phase.
4. The installation file is distributed from the distributor to the system-installer.
 - a. The installation file is temporarily stored. Depending on the accessibility of the this temporary storage there is a medium (internal) to high (public) risk of modification of the installation file in this phase.
5. The installation file is downloaded from the Bosch Security Systems website to a system-installer.
 - a. The installation file is distributed over the internet. Due to the point-to-point connection there is little to medium risk of modification of the installation file in this phase.

Recommendation

To reduce the risk of modification Bosch Security Systems strongly recommends that system-installers download the software installation file directly from the Bosch Security Systems website.

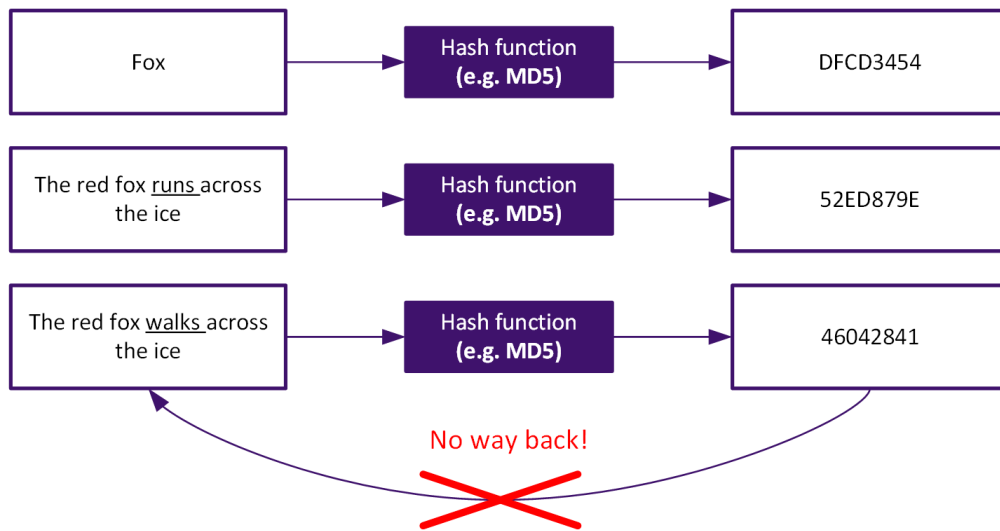
2.2 Solution

Downloading the installation file from the website directly does not guarantee the software is delivered as it has been generated by the engineering team. This section explains what concepts are used to check the installation file.

Checksum and Hashes

Based on a hash, or checksum, the integrity of information can be verified.

A hash algorithm is used to generate a fixed length key which relates directly to a unique word, or in this case, an installation file. Hashing is a one way function, there is no way to go back from the hashed value to the original value.



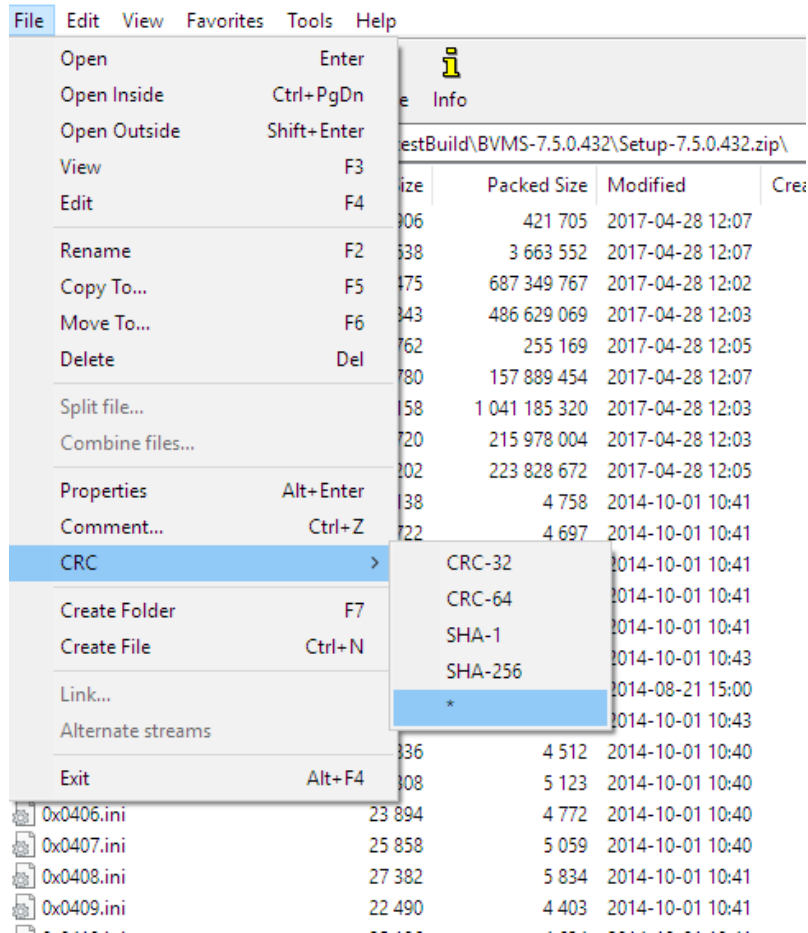
As a result, every time the word "Fox" is inserted into the hash function, the output will be exactly the same (DFCD3454). Using the installation file as an example, the same concept is applied: when the file is processed, a hash value is calculated. When the file is modified, the calculated hash value will also change. When the original (stored) hash value and the calculated, current, hash value, are compared, they will not match. This will mean the original installation file has been modified.

3 Verifying the download

This section describes how to verify if the installation file matches the expected output. The 7-Zip, open source, file compression utility includes the functionality to check the integrity of a file.

Download 7-Zip

Open the software installation zip, which can be downloaded from the Bosch Security Systems website. In 7-Zip click **File > CRC > ***



The results can be compared with the checksum displayed on the [Bosch downloadstore](#).

Platform	Version	Firmware URL	Checksum	Release note
BVMS	8.0.0	BVMS_8.0_Software_Setup_8.0.0.329_at_35502615051.zip	B4C8162B0618057AC3E47E6B8845EB72D6A08F96	BVMS_8.0_Release_Note_enUS_35168519307.pdf
BVMS	8.0.0	BVMS_Viewer_8.0_Software_Setup_8.0.0.329_at_35502695179.zip	90FA3B510338DD1AD5F54254541D2167B3531DC1	BVMS_Viewer_8.0_Release_Note_enUS_35117537419.pdf
BVMS	7.5.0	Software_Setup_7.5.0.432_at_28203230279.zip		
BVMS	7.5.0	Viewer_7.5_Software_Setup_7.5.0.432_at_28203799987.zip		
BVMS	7.0.0	Software_Setup_7.0.0.223_at_23721243275.zip		
BVMS	6.5.0	Software_Setup_6.5.0.325_at_22547369227.zip		
BVMS	6.0.0	Software_Setup_6.0.0.453_at_20710863115.zip		
BVMS	5.5.5	Software_Setup_5.5.5.258_at_18862887563.zip		

Example of checksums in a ZIP file

The checksums for a typical installation ZIP file as they appear in the 7-Zip application:

```
-----  
7-Zip  
-----  
Folders: 36  
Files: 201  
Size: 2903784133 bytes (2769MB)  
CRC32 checksum for data: 43CB44A5  
CRC32 checksum for data and names: 827EAA3F  
CRC64 checksum for data: 248DED357F75E492  
CRC64 checksum for data and names: 9CA3603E1BD6A7E9  
SHA256 checksum for data: 660C90899D1078D86CD5C52ED9D8777DAB2923D998CA3E389F94B03E5C82787B  
SHA256 checksum for data and names: FE59F07FCF2318A9E390633C98308E2608FE6B5103DE55C752B56FB08C2AA737  
SHA1 checksum for data: E35D7879667B0675C0DEDFBCC607261B2438D20A  
SHA1 checksum for data and names: 83F6022D2B576340E7E11B6BFEE5D5A2AB085BB8  
BLAKE2sp checksum for data: 5BF1499C2C0DA25253928C16BC643AC6DA978C03D1D8BE79042BF7FE4E41AB0D  
BLAKE2sp checksum for data and names: 0E6D7C02601E3F9F7B329EBC2413D6AEB9C040835BABAB1804C0C4FFFE6C65B64  
-----  
OK  
-----
```