Security Certification

Device Testing

Rama Krishna Majety

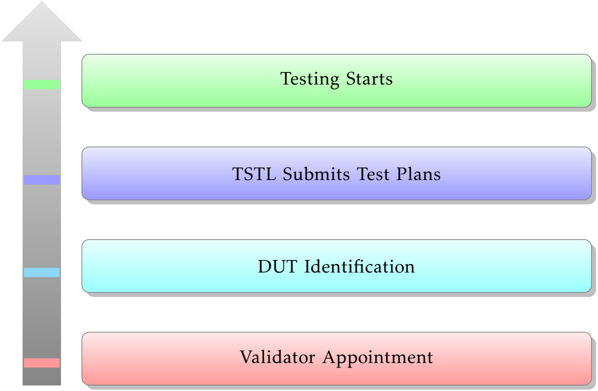
National Centre For Communication Security, Bengaluru

19th Mar, 2025

Topics for discussion

- Introduction to Security Certification
- Device and Software Identification
- Encrypted and open images of OS.
- Some Examples
- Integrity checking Hashing mechanism - a comparison.

Security Certification Methodology



Testing Starts

TSTL Submits Test Plans

DUT Identification

Validator Appointment

Security Testing – Device

Networking Devices run OS for providing the Routing, WiFi access etc.

- OpenWRT [1], ONIE [2], Ruckus, [3]
- Cisco IOS, Junos, IPOS …

Device: Software (Application, Firmware, OS etc.,) running on Hardware to provide the functionality of Router, WiFi CPE, ONT, OLT, Firewall etc.

[1] https://openwrt.org/start

[2] https://opencomputeproject.github.io/onie/

[3] https://support.ruckuswireless.com/software

Main Model and Associated Models

- Main model runs same software as it is run in Associated Models.
- Associated models have similar hardware or may be of lesser capacity.
- Associated Model never will have higher capacity or additional feature than those of Main Model.

Relating Main model with Associated Model

- Firmware [4] has to be same.
- Should be derivable from that of Main Model by dropping some modules or with a different chipset.

[4] Networking OS, Application, Firmware, all components available in Device

Firware of Networking Devices

- Firmware repositories are available over Internet, to authorised users.
- Hash and version are declared for verification.
- Device shall support Verifying the integrity of the firmware being used for upgrade and while rebooting.
- Supporting applications and public keys are also hosted by OEMs for handling firmware.

Networking OS

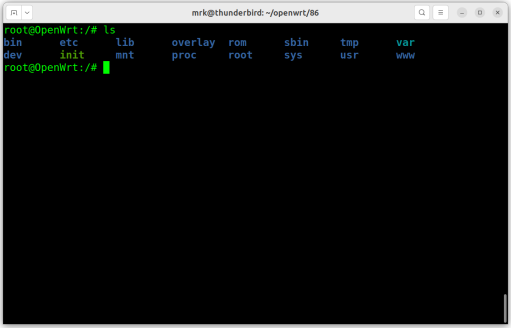
- Linux like OS running router as an Application.
- Software, with version/release details, is available for authorised users.
- Upgrade or Recovery of Devices also use these images.
- Un-encrypted images available as .compressed file (tar.gz)
- Encrypted images with Vendor specific formats.

Un encrypted OS Images

Openwrt OS

openwrt-24.10.0-x86-64-generic-ext4-combined.img.gz Extracted before installing in the Device.

File System



```
root@OpenWrt:/# ls
bin       etc       lib       overlay  rom      sbin     tmp      var
dev       init      mnt       proc     root     sys      usr      www
root@OpenWrt:/# 
```

Public and Private Key Encryption

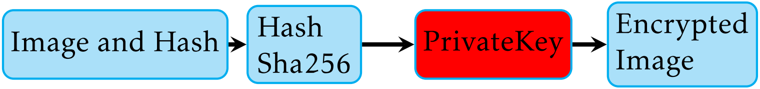
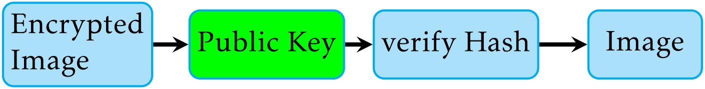


Image and Hash → Hash Sha256 → PrivateKey → Encrypted Image

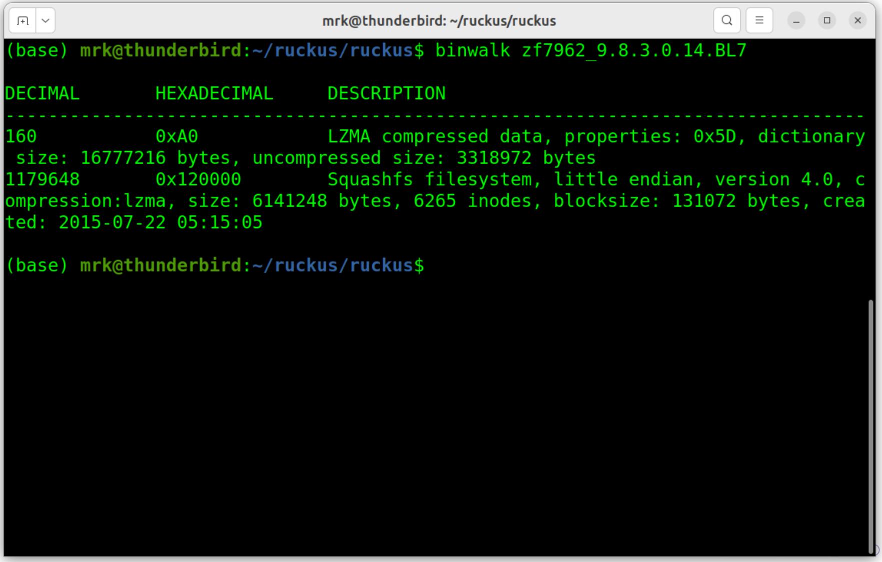


Encrypted Image → Public Key → verify Hash → Image

Tools used for verification

- openssl
- certutils
- md5sum sha256sum etc.
- hexedit, hexdump, xxd, binwalk for inspecting bin files.

checking image file with binwalk

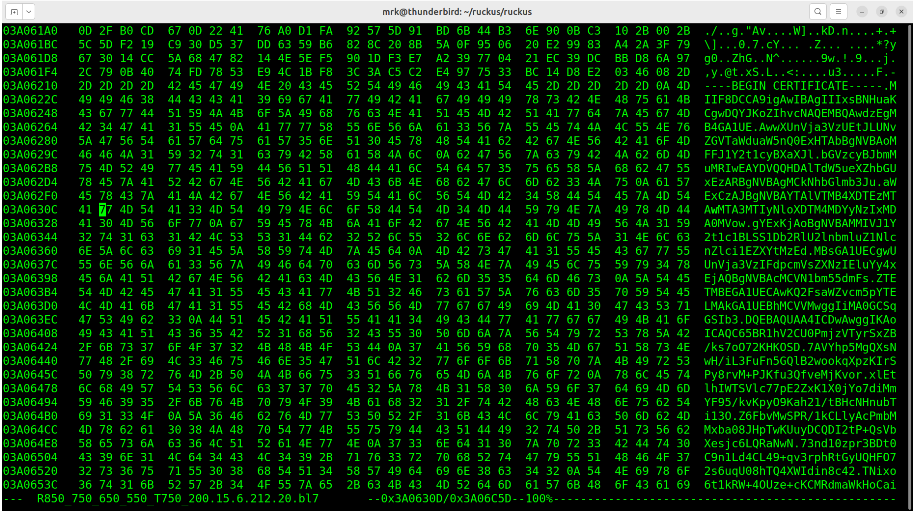


```
(base) mrk@thunderbird:~/ruckus/ruckus$ binwalk zf7962_9.8.3.0.14.BL7

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
160           0xA0            LZMA compressed data, properties: 0x5D, dictionary
 size: 16777216 bytes, uncompressed size: 3318972 bytes
1179648       0x120000        Squashfs filesystem, little endian, version 4.0, c
ompression:lzma, size: 6141248 bytes, 6265 inodes, blocksize: 131072 bytes, crea
ted: 2015-07-22 05:15:05

(base) mrk@thunderbird:~/ruckus/ruckus$
```

Where is Public Key - hexedit



mrk@thunderbird: ~/ruckus/ruckus

```
03A061A0   0D 2F B0 CD  67 0D 22 41  76 A0 D1 FA  92 57 5D 91  BD 6B 44 B3  6E 90 0B C3  10 2B 00 2B  ./..g."Av....W]..kD.n....+.+
03A061BC   5C 5D F2 19  C9 30 D5 37  DD 63 59 B6  82 8C 20 8B  5A 0F 95 06  20 E2 99 83  A4 2A 3F 79  \]...0.7.cY... .Z... ....*?y
03A061D8   67 30 14 CC  5A 68 47 82  14 4E 5E F5  90 1D F3 E7  A2 39 77 04  21 EC 39 DC  BB D8 6A 97  g0..ZhG..N^......9w.!.9...j.
03A061F4   2C 79 0B 40  74 FD 78 53  E9 4C 1B F8  3C 3A C5 C2  E4 97 75 33  BC 14 D8 E2  03 46 08 2D  ,y.@t.xS.L..<:....u3.....F.-
03A06210   2D 2D 2D 2D  42 45 47 49  4E 20 43 45  52 54 49 46  49 43 41 54  45 2D 2D 2D  2D 2D 0A 4D  ----BEGIN CERTIFICATE-----.M
03A0622C   49 49 46 38  44 43 43 41  39 69 67 41  77 49 42 41  67 49 49 49  78 73 42 4E  48 75 61 4B  IIF8DCCA9igAwIBAgIIIxsBNHuaK
03A06248   43 67 77 44  51 59 4A 4B  6F 5A 49 68  76 63 4E 41  51 45 4D 42  51 41 77 64  7A 45 67 4D  CgwDQYJKoZIhvcNAQEMBQAwdzEgM
03A06264   42 34 47 41  31 55 45 0A  41 77 77 58  55 6E 56 6A  61 33 56 7A  55 45 74 4A  4C 55 4E 76  B4GA1UE.AwwXUnVja3VzUEtJLUNv
03A06280   5A 47 56 54  61 57 64 75  61 57 35 6E  51 30 45 78  48 54 41 62  42 67 4E 56  42 41 6F 4D  ZGVTaWduaW5nQ0ExHTAbBgNVBAoM
03A0629C   46 46 4A 31  59 32 74 31  63 79 42 58  61 58 4A 6C  0A 62 47 56  7A 63 79 42  4A 62 6D 4D  FFJ1Y2t1cyBXaXJl.bGVzcyBJbmM
03A062B8   75 4D 52 49  77 45 41 59  44 56 51 51  48 44 41 6C  54 64 57 35  75 65 58 5A  68 62 47 55  uMRIwEAYDVQQHDAlTdW5ueXZhbGU
03A062D4   78 45 7A 41  52 42 67 4E  56 42 41 67  4D 43 6B 4E  68 62 47 6C  6D 62 33 4A  75 0A 61 57  xEzARBgNVBAgMCkNhbGlmb3Ju.aW
03A062F0   45 78 43 7A  41 4A 42 67  4E 56 42 41  59 54 41 6C  56 54 4D 42  34 58 44 54  45 7A 4D 54  ExCzAJBgNVBAYTAlVTMB4XDTEzMT
03A0630C   41 77 4D 54  41 33 4D 54  49 79 4E 6C  6F 58 44 54  4D 34 4D 44  59 79 4E 7A  49 78 4D 44  AwMTA3MTIyNloXDTM4MDYyNzIxMD
03A06328   41 30 4D 56  6F 77 0A 67  59 45 78 4B  6A 41 6F 42  67 4E 56 42  41 4D 4D 49  56 4A 31 59  A0MVow.gYExKjAoBgNVBAMMIVJ1Y
03A06344   32 74 31 63  31 42 4C 53  53 31 44 62  32 52 6C 55  32 6C 6E 62  6D 6C 75 5A  31 4E 6C 63  2t1c1BLSS1Db2RlU2lnbmluZ1Nlc
03A06360   6E 5A 6C 63  69 31 45 5A  58 59 74 4D  7A 45 64 0A  4D 42 73 47  41 31 55 45  43 67 77 55  nZlci1EZXYtMzEd.MBsGA1UECgwU
03A0637C   55 6E 56 6A  61 33 56 7A  49 46 64 70  63 6D 56 73  5A 58 4E 7A  49 45 6C 75  59 79 34 78  UnVja3VzIFdpcmVsZXNzIEluYy4x
03A06398   45 6A 41 51  42 67 4E 56  42 41 63 4D  43 56 4E 31  62 6D 35 35  64 6D 46 73  0A 5A 54 45  EjAQBgNVBAcMCVN1bm55dmFs.ZTE
03A063B4   54 4D 42 45  47 41 31 55  45 43 41 77  4B 51 32 46  73 61 57 5A  76 63 6D 35  70 59 54 45  TMBEGA1UECAwKQ2FsaWZvcm5pYTE
03A063D0   4C 4D 41 6B  47 41 31 55  45 42 68 4D  43 56 56 4D  77 67 67 49  69 4D 41 30  47 43 53 71  LMAkGA1UEBhMCVVMwggIiMA0GCSq
03A063EC   47 53 49 62  33 0A 44 51  45 42 41 51  55 41 41 34  49 43 44 77  41 77 67 67  49 4B 41 6F  GSIb3.DQEBAQUAA4ICDwAwggIKAo
03A06408   49 43 41 51  43 36 35 42  52 31 68 56  32 43 55 30  50 6D 6A 7A  56 54 79 72  53 78 5A 42  ICAQC65BR1hV2CU0PmjzVTyrSxZB
03A06424   2F 6B 73 37  6F 4F 37 32  4B 48 4B 4F  53 44 0A 37  41 56 59 68  70 35 4D 67  51 58 73 4E  /ks7oO72KHKOSD.7AVYhp5MgQXsN
03A06440   77 48 2F 69  4C 33 46 75  46 6E 35 47  51 6C 42 32  77 6F 6F 6B  71 58 70 7A  4B 49 72 53  wH/iL3FuFn5GQlB2wookqXpzKIrS
03A0645C   50 79 38 72  76 4D 2B 50  4A 4B 66 75  33 51 66 76  65 4D 6A 4B  76 6F 72 0A  78 6C 45 74  Py8rvM+PJKfu3QfveMjKvor.xlEt
03A06478   6C 68 49 57  54 53 56 6C  63 37 37 70  45 32 5A 78  4B 31 58 30  6A 59 6F 37  64 69 4D 6D  lhIWTSVlc77pE2ZxK1X0jYo7diMm
03A06494   59 46 39 35  2F 6B 76 4B  70 79 4F 39  4B 61 68 32  31 2F 74 42  48 63 4E 48  6E 75 62 54  YF95/kvKpyO9Kah21/tBHcNHnubT
03A064B0   69 31 33 4F  0A 5A 36 46  62 76 4D 77  53 50 52 2F  31 6B 43 4C  6C 79 41 63  50 6D 62 4D  i13O.Z6FbvMwSPR/1kCLlyAcPmbM
03A064CC   4D 78 62 61  30 38 4A 48  70 54 77 4B  55 75 79 44  43 51 44 49  32 74 50 2B  51 73 56 62  Mxba08JHpTwKUuyDCQDI2tP+QsVb
03A064E8   58 65 73 6A  63 36 4C 51  52 61 4E 77  4E 0A 37 33  6E 64 31 30  7A 70 72 33  42 44 74 30  Xesjc6LQRaNwN.73nd10zpr3BDt0
03A06504   43 39 6E 31  4C 64 34 43  4C 34 39 2B  71 76 33 72  70 68 52 74  47 79 55 51  48 46 4F 37  C9n1Ld4CL49+qv3rphRtGyUQHFO7
03A06520   32 73 36 75  71 55 30 38  68 54 51 34  58 57 49 64  69 6E 38 63  34 32 0A 54  4E 69 78 6F  2s6uqU08hTQ4XWIdin8c42.TNixo
03A0653C   36 74 31 6B  52 57 2B 34  4F 55 7A 65  2B 63 4B 43  4D 52 64 6D  61 57 6B 48  6F 43 61 69  6t1kRW+4OUze+cKCMRdmaWkHoCai
---  R850_750_650_550_T750_200.15.6.212.20.bl7       --0x3A0630D/0x3A06C5D--100%------------------------------------------------------------
```

Weak and Strong Hash functions

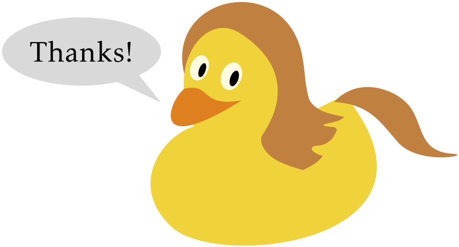
- md5 and sha1
- sha256, 512

MD5 Collision

- Created by Ronald Rivest in 1991
- 128 Bit length
- Collision were suspected during 1994.
- Collision was successfully demonstrated during 2004.

SHA - 1 and higher

- Deprecated by NIST in 2011.
-
- Collisions are possible and demonstrated.
- SHA-2 family of hash algorithms: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, and SHA-512/256


Thanks!