

ELF Code Signing

chihchun

2005/01/22

Bsign

Corruption & intrusion detection using embedded hashes

- Ensuring Integrity
- Ensuring Authenticity

Functions

- **This package embeds secure hashes (SHA1) and digital signatures (GNU Privacy Guard) into files for verification and authentication.**
- **Formats**
 - **executables**
 - **kernel modules**
 - **shared and static link libraries.**

integrity checker

- tripwire.org
- integrit.sf.net

Mobile Code

- **Microsoft Authenticode Technology**
 - .cab files
 - .cat files
 - .ctl files
 - .dll files
 - .exe files
 - .ocx
- **Sun Java Code Signing**
 - Jar files

Usage

```
chihchun@kalug: /home/chihchun/workspace/bsign
檔案(F) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)
chihchun@kalug:~/workspace/bsign$ cp /bin/ls .
chihchun@kalug:~/workspace/bsign$ md5sum ls /bin/ls
cel243c8b432abc494b01ff36ea909ef  ls
cel243c8b432abc494b01ff36ea909ef  /bin/ls
chihchun@kalug:~/workspace/bsign$ gpg --list-keys
/home/chihchun/.gnupg/pubring.gpg
-----
pub 1024D/5A944530 2005-01-30 demo user <nobody@chroot.org>
sub 1024g/800507F8 2005-01-30

chihchun@kalug:~/workspace/bsign$ bsign -s ./ls

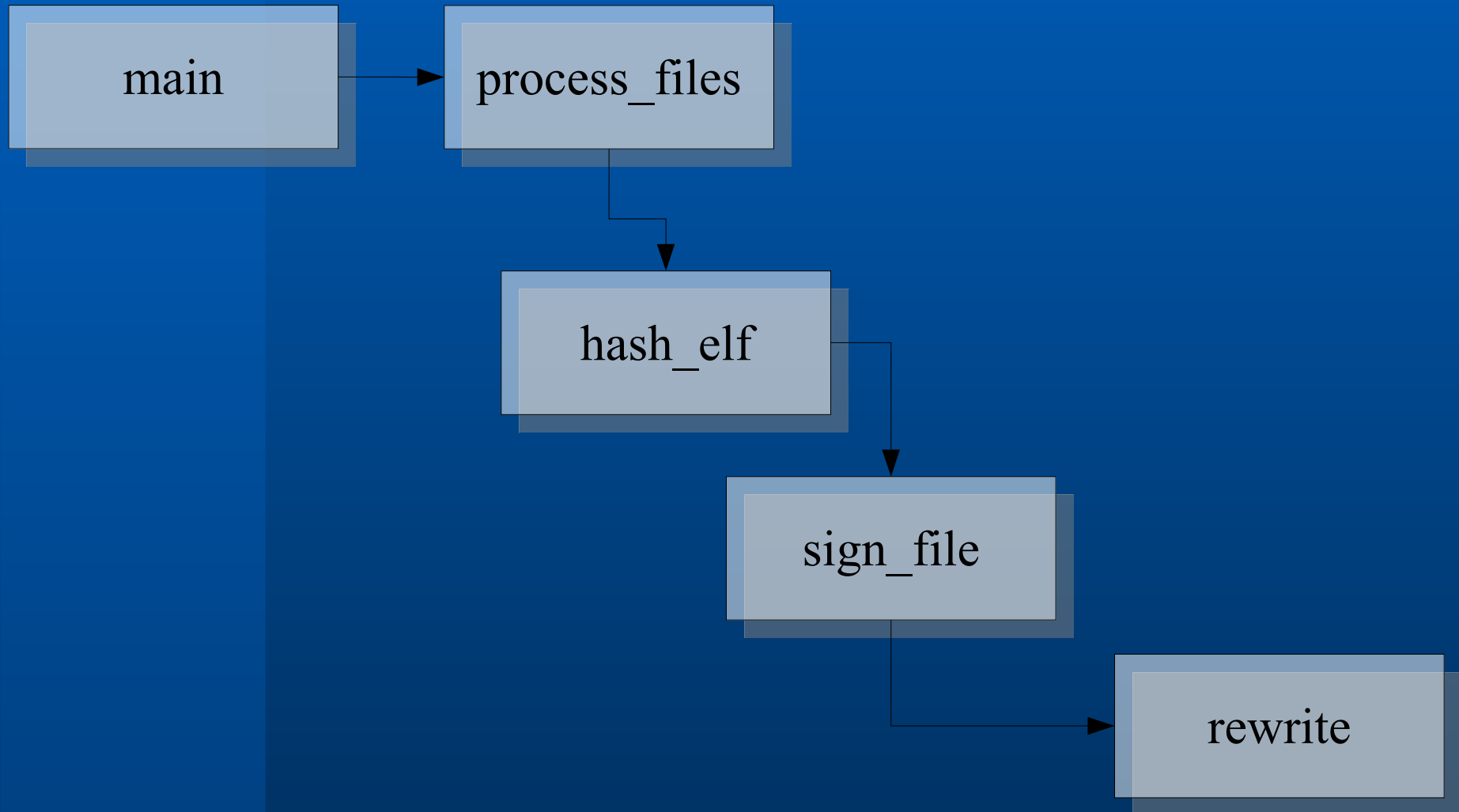
Enter pass phrase:
chihchun@kalug:~/workspace/bsign$ md5sum ls /bin/ls
9ae255356c9d275a96e0f8d67a5e8a89  ls
cel243c8b432abc494b01ff36ea909ef  /bin/ls
chihchun@kalug:~/workspace/bsign$ ./ls
bsign-0.4.5  bsign_0.4.5.dsc  bsign_0.4.5.tar.gz  ls
chihchun@kalug:~/workspace/bsign$ bsign ./ls
bsign: good hash found in './ls'.
chihchun@kalug:~/workspace/bsign$
```

```
chihchun@kalug: /home/chihchun/workspace/bsign
檔案(F) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)
chihchun@kalug:~/workspace/bsign$ readelf -S ./1s > 1
chihchun@kalug:~/workspace/bsign$ readelf -S /bin/1s > 2
chihchun@kalug:~/workspace/bsign$ diff -u 2 1
--- 2    2005-01-31 02:08:49.000000000 +0800
+++ 1    2005-01-31 02:08:45.000000000 +0800
@@ -1,4 +1,4 @@
-There are 25 section headers, starting at offset 0x124c4:
+There are 26 section headers, starting at offset 0x124d1:

Section Headers:
  [Nr] Name              Type              Addr              Off              Size              ES Flg Lk  Inf A
 1
@@ -25,8 +25,9 @@
  [20] .dtors                PROGBITS          0805a264 012264 000008 00  WA  0  0
 4
  [21] .jcr                  PROGBITS          0805a26c 01226c 000004 00  WA  0  0
 4
  [22] .got                  PROGBITS          0805a270 012270 000184 04  WA  0  0
 4
- [23] .bss                  NOBITS            0805a400 012400 0003b0 00  WA  0  0 3
 2
- [24] .shstrtab             STRTAB            00000000 012400 0000c3 00           0  0
 1
+ [23] .bss                  NOBITS            0805a400 012400 0003e5 00  WA  0  0 3
```

```
chihchun@kalug: /home/chihchun/workspace/bsign
檔案(F) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)
Section Headers:
  [Nr] Name                               Type             Addr             Off             Size            ES Flg Lk Inf A
  1
@@ -25,8 +25,9 @@
  [20] .dtors                                 PROGBITS         0805a264         012264          000008          00  WA  0  0
  4
  [21] .jcr                                  PROGBITS         0805a26c         01226c          000004          00  WA  0  0
  4
  [22] .got                                  PROGBITS         0805a270         012270          000184          04  WA  0  0
  4
- [23] .bss                                 NOBITS           0805a400         012400          0003b0          00  WA  0  0 3
  2
- [24] .shstrtab                          STRTAB           00000000         012400          0000c3          00                   0  0
  1
+ [23] .bss                                 NOBITS           0805a400         012400          0003e5          00  WA  0  0 3
  2
+ [24] .shstrtab                          STRTAB           00000000         012400          0000dd          00                   0  0
  1
+ [25] signature                          LOUSER+736967   00000000         0128e1          000200          00                   0  0
  1
Key to Flags:
  W (write), A (alloc), X (execute), M (merge), S (strings)
  I (info), L (link order), G (group), x (unknown)
chihchun@kalug:~/workspace/bsign$
```


Source Code



References

- **Marc Singer <elf at debian.org>**
 - <ftp://ftp.buici.com/pub/bsign>
- **Microsoft Authenticode**
 - http://msdn.microsoft.com/library/default.asp?url=/workshop/security/authcode/authenticode_node_en_try.asp
- **Java Code Signing**
 - <http://java.sun.com/security/codesign>