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.**

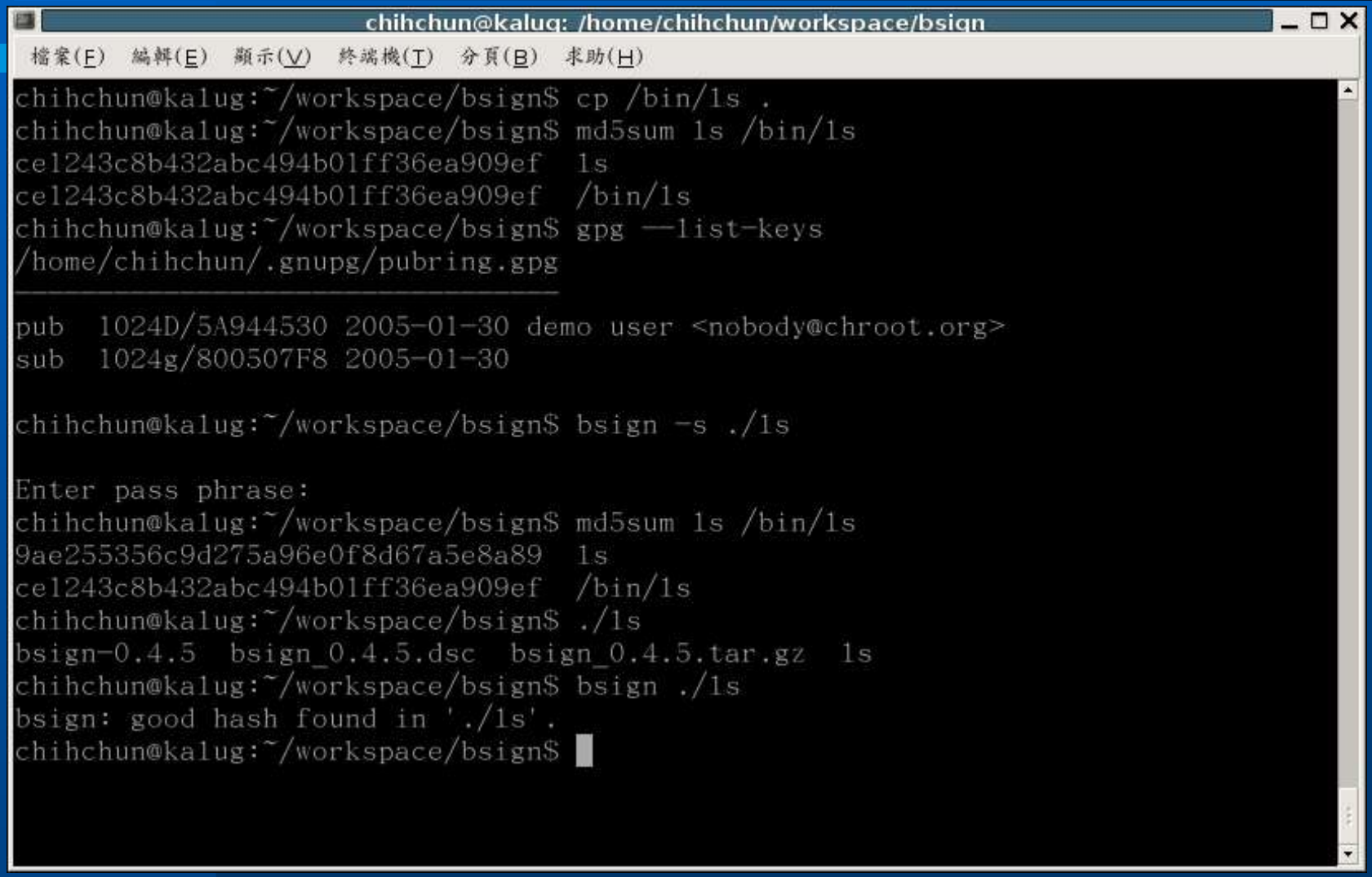
integrity checker

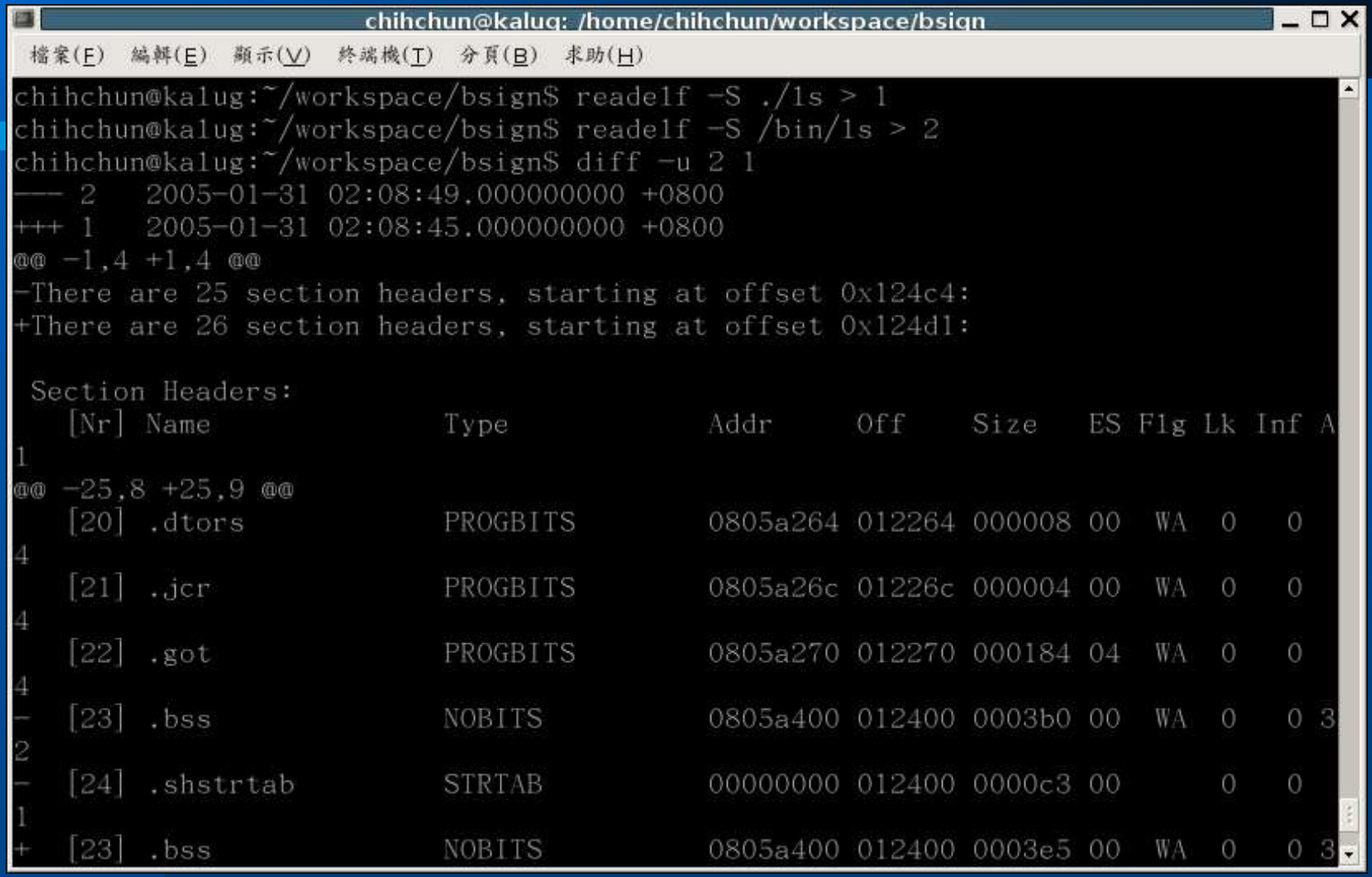
- **tripwire.org**
- **integrit.sf.net**

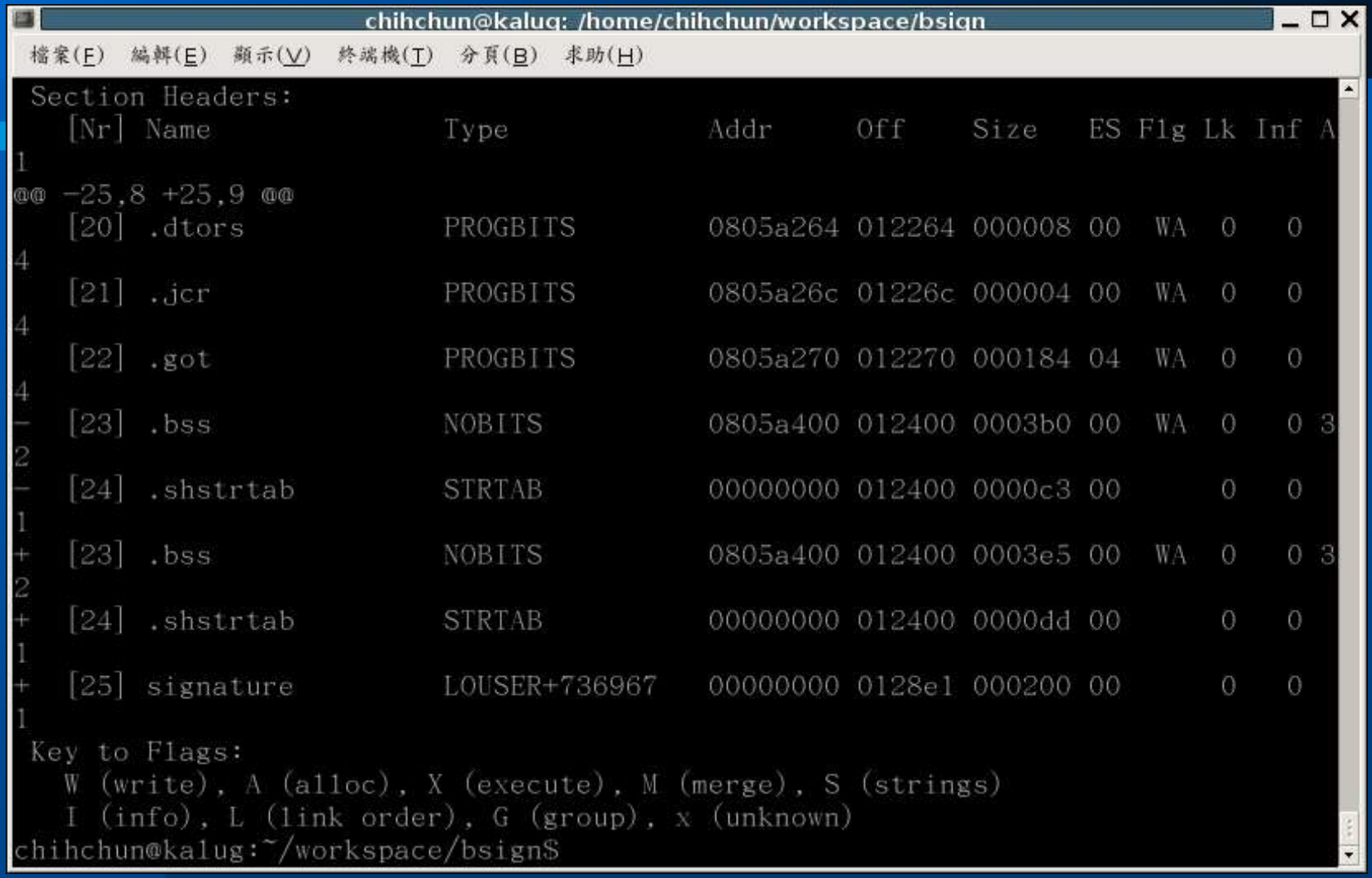
Mobile Code

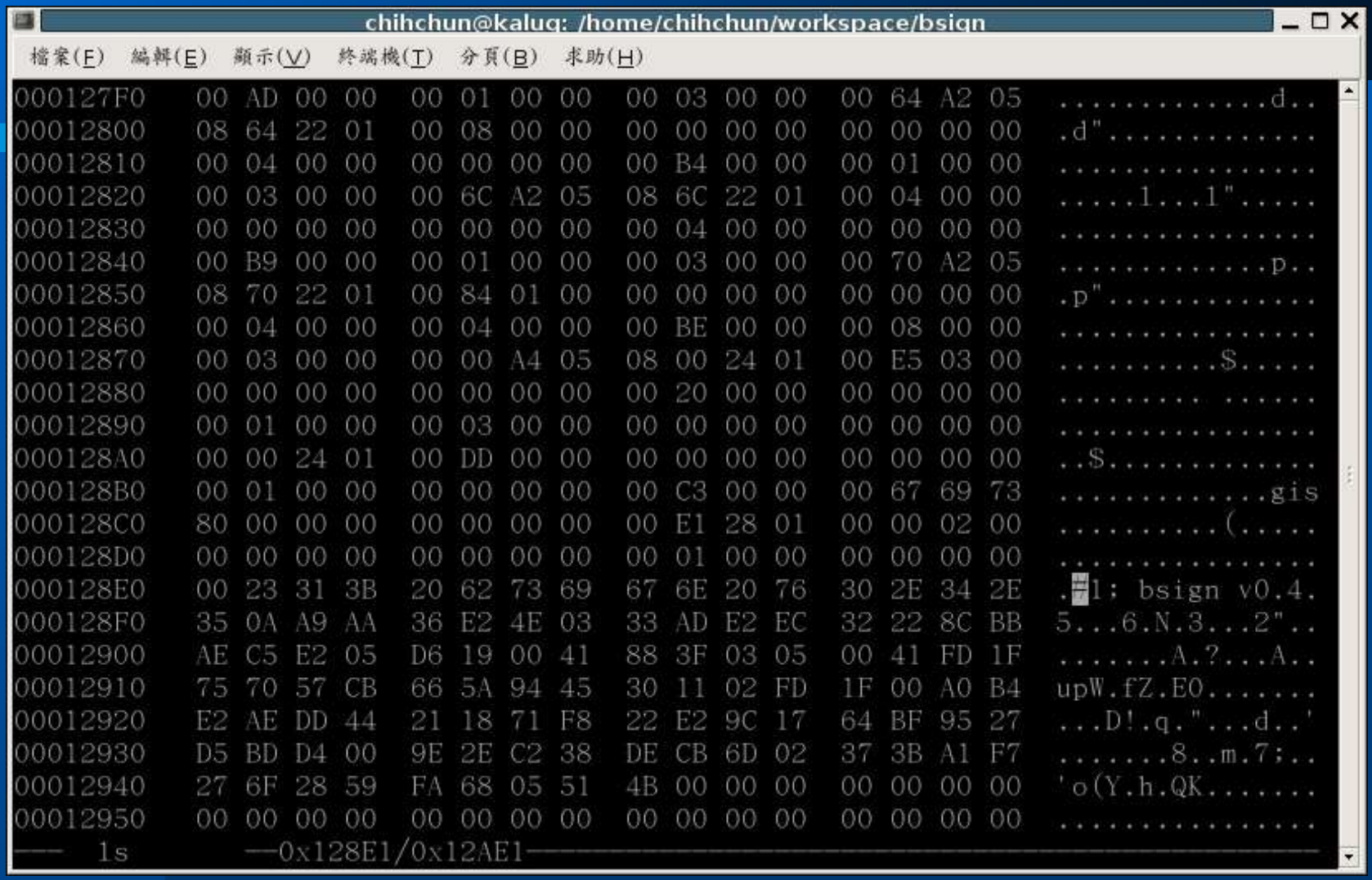
- **Microsoft Authenticode Technology**
  - **.cab files**
  - **.cat files**
  - **.ctl files**
  - **.dll files**
  - **.exe files**
  - **.ocx**
- **Sun Java Code Signing**
  - **Jar files**

Usage

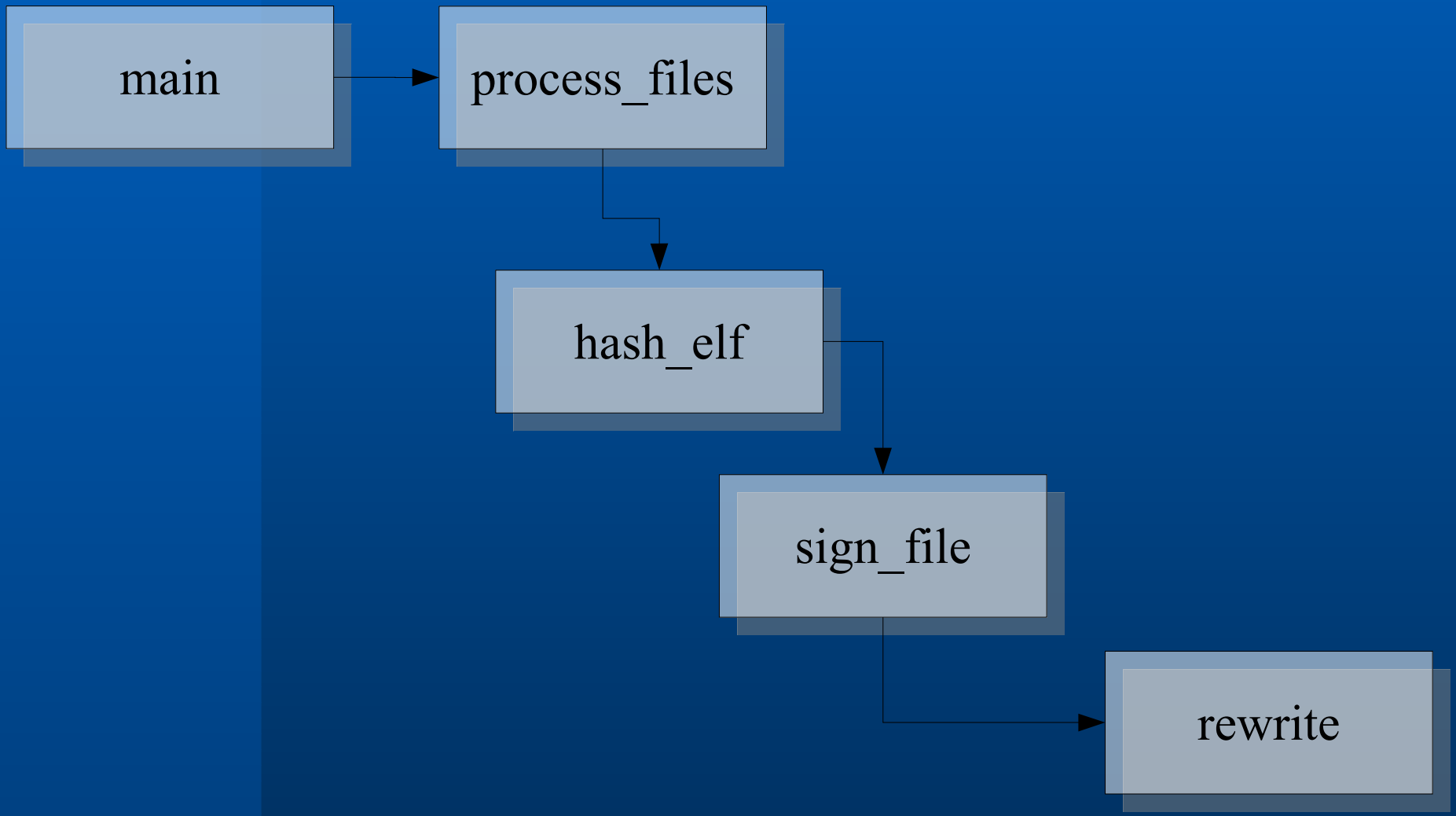

chihchun@kalug: /home/chihchun/workspace/bsign
檔案(F) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)
chihchun@kalug:~/workspace/bsign$ cp /bin/ls .
chihchun@kalug:~/workspace/bsign$ md5sum ls /bin/ls
ce1243c8b432abc494b01ff36ea909ef ls
ce1243c8b432abc494b01ff36ea909ef /bin/ls
chihchun@kalug:~/workspace/bsign$ gpg --list-keys
/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
ce1243c8b432abc494b01ff36ea909ef /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 ./ls > 1
chihchun@kalug:~/workspace/bsign$ readelf -S /bin/ls > 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$


chihchun@kaluq: /home/chihchun/workspace/bsign
檔案(F) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)
000127F0 00 AD 00 00 00 01 00 00 00 03 00 00 00 64 A2 05 .....d..
00012800 08 64 22 01 00 08 00 00 00 00 00 00 00 00 00 00 .d".....
00012810 00 04 00 00 00 00 00 00 00 B4 00 00 00 01 00 00 .....
00012820 00 03 00 00 00 6C A2 05 08 6C 22 01 00 04 00 00 .....l..l".....
00012830 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 00 .....
00012840 00 B9 00 00 00 01 00 00 00 03 00 00 00 70 A2 05 .....p..
00012850 08 70 22 01 00 84 01 00 00 00 00 00 00 00 00 00 .p".....
00012860 00 04 00 00 00 04 00 00 00 BE 00 00 00 08 00 00 .....
00012870 00 03 00 00 00 00 A4 05 08 00 24 01 00 E5 03 00 .....$.....
00012880 00 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 ....
00012890 00 01 00 00 00 03 00 00 00 00 00 00 00 00 00 00 .....
000128A0 00 00 24 01 00 DD 00 00 00 00 00 00 00 00 00 00 ..$.....
000128B0 00 01 00 00 00 00 00 00 00 C3 00 00 00 67 69 73 .....gis
000128C0 80 00 00 00 00 00 00 00 00 E1 28 01 00 00 02 00 .....(.....
000128D0 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 .....
000128E0 00 23 31 3B 20 62 73 69 67 6E 20 76 30 2E 34 2E .#1; bsign v0.4.
000128F0 35 0A A9 AA 36 E2 4E 03 33 AD E2 EC 32 22 8C BB 5...6.N.3...2"..
00012900 AE C5 E2 05 D6 19 00 41 88 3F 03 05 00 41 FD 1F .....A.?...A..
00012910 75 70 57 CB 66 5A 94 45 30 11 02 FD 1F 00 A0 B4 upW.fZ.E0.....
00012920 E2 AE DD 44 21 18 71 F8 22 E2 9C 17 64 BF 95 27 ...D!.q."...d..'
00012930 D5 BD D4 00 9E 2E C2 38 DE CB 6D 02 37 3B A1 F7 .....8..m.7;..
00012940 27 6F 28 59 FA 68 05 51 4B 00 00 00 00 00 00 00 'o(Y.h.QK.....
00012950 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
--- 1s --0x128E1/0x12AE1---

Surce 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