Programa de Becas de Formación en Seguridad Informática Coordinación de Seguridad de la Información UNAM-CERT Administración y seguridad en redes

Práctica Colision MD5 30/09/2018

David Martin Jimenez/Jesus Pacheco/Servando Lopez

## Colisión MD5

Para esta practica se uso el método de Peter Sellinger, el cual consiste en hacer un programa ejecutable con código "esquizofrenico" el cual incluye dos códigos con contenido diferente, y basándose en la función de MD5 se elige activar uno u otro código ya que la función de MD5 permite que los hashes arrojados sean iguales y nos da una ventana de 128 bytes en medio de los bloques elegidos para conformar el hash.

El programa que escribí es el siguiente:

```
#include <stdio.h>
main_good() {
    printf("hola, mundo!\n");
    return 0;
}
main_evil() {
    printf("ya te atrapo la vibora!!!\n");
    printf("Erasing hard drive...");
    printf("1Gb...");
    printf("2Gb...");
    printf(" caiste!\nbuendia.\n");
    return 0;
}
```



Programa de Becas de Formación en Seguridad Informática Coordinación de Seguridad de la Información UNAM-CERT Administración y seguridad en redes

Utilize la herramienta evilize del mismo autor, la descomprimí y compile.

```
File Edit View Search Terminal Help

root@Kali: -/Downloads*
root@Kali: -/Downloads# ls
evilize-0.2.tar.gz libssli,0.0 1.0.1t-1+deb8u7_amd64.deb
lainzine04.pdf tor-browser-linux64-7.0.8_en-US.tar.xz
root@Kali: -/Downloads# tar zxf evilize-0.2.tar.gz
root@Kali: -/Downloads# tar zxf evilize-0.2.tar.gz
root@Kali: -/Downloads# ls
evilize-0.2.tar.gz tor-browser-linux64-7.0.8_en-US.tar.xz
lainzine04.pdf
root@Kali: -/Downloads# cd evilize-0.2# make
gcc -03 -Wall -DSTDC_HEADERS -g -DMD5COLL_VERSION=\"0.1s\" -DVERSION=\"0.2\" -
c -0 evilize.0 evilize.c
gcc -03 -Wall -DSTDC_HEADERS -g -DMD5COLL_VERSION=\"0.1s\" -DVERSION=\"0.2\" -
c -0 md5coll_tib.o md5coll_tib.o -0 evilize
gcc -03 -Wall -DSTDC_HEADERS -g -DMD5COLL_VERSION=\"0.1s\" -DVERSION=\"0.2\" -
c -0 md5coll_tib.o md5coll_tib.o -0 evilize
gcc -03 -Wall -DSTDC_HEADERS -g -DMD5COLL_VERSION=\"0.1s\" -DVERSION=\"0.2\" -
c -0 md5coll_to md5coll_tib.o -0 md5coll_VERSION=\"0.1s\" -DVERSION=\"0.2\" -
c -0 md5coll.o md5coll_tib.o -0 md5coll_VERSION=\"0.1s\" -DVERSION=\"0.2\" -
c -0 md5coll.o md5coll_tib.o -0 md5coll_
gcc -03 -Wall -DSTDC_HEADERS -g -DMD5COLL_VERSION=\"0.1s\" -DVERSION=\"0.2\" -
c -0 md5coll.o md5coll_tib.o -0 md5coll_
gcc -03 -Wall -DSTDC_HEADERS -g -DMD5COLL_VERSION=\"0.1s\" -DVERSION=\"0.2\" -
c -0 md5coll.o md5coll_tib.o -0 md5coll_
gcc -03 -Wall -DSTDC_HEADERS -g -DMD5COLL_VERSION=\"0.1s\" -DVERSION=\"0.2\" -
c -0 goodevil.o goodevil.c
root@Kali:-/Downloads/evilize-0.2#
```

Compile mi código y lo uní al objeto *goodevil* para posteriormente lograr un un vector de inizializacion.



Programa de Becas de Formación en Seguridad Informática Coordinación de Seguridad de la Información UNAM-CERT

Administración y seguridad en redes Alliciack-rig Tokali Folums Tokethunter of Most Visited V root@Kali: File Edit View Search Terminal Mall: "# echon David Martin and Yu's algorithm. You can find his original implementation David Martin ot@Kali:-# nes root@Kali: ~/Downloads/evilize-0.2 Edit View Search Terminal Help :~/Downloads/evilize-0.2# gcc hola\_vibora.c goodevil.o -o hola\_vibora :~/Downloads/evilize-0.2# ./evilize hola\_vibora -i Initial vector: 0x01117007 0x766d3d4d 0xb5a1d3da 0x5dafad26 :~/Downloads/evilize-0.2# ./md5coll 0x01117007 0x766d3d4d 0xb5a1d3da 0x 5dafad26 > init.txt Progress: 103.131.308.15 (done) ect file "goodevil.o" :~/Downloads/evilize-0:2# al top-level function main(), write two separate in level fun ad link against goodevil.o. For example: and to create an initialization vector:

## Se creo una colision de MD5

```
re is based on Patr
                                                     i:~# echo "David Martin"
                                                                                                                                                                                                   ation here.
                                     David Martin
                                                      :~#
 ge instructions:
 indows users the
                                                                                                                                                                                                  nes of execu
                                                                                root@Kali: ~/Downloads/evilize.0 2
                                                                                                                                                                                - 0 X
 ke", you must har
                                  File Edit View Search Terminal Help
 ck the archive an Random seed: 1409111038
r zxf evilize-0.2.ta unsigned int m0[32] = {
    evilize-0.2.ta unsigned int m0[32] = {
        evilize-0.2.ta unsigned int m0[32] = {
            0x45826c7d, 0x731662a8, 0x13596900, 0xa080318f, 0x4d17e8ed, 0x38f2fd9d, 0xc15694e1, 0x507f8a34, 0x05346d51, 0x20737fff, 0x8564a99f, 0x10a96f77, 0x55bfbef3, 0x885b5ffe, 0x11d6cd90, 0xf3d867ef, 0x65f9154c, 0xbe2b8389, 0xcb7dcbf6, 0xcdellcaf, 1_evil(). See the file 0x160896cb, 0x1cb4ccf1, 0x56a1bd14, 0xe04cedd0, pile your program 0xbabaefe5, 0xcc357360, 0xbf380d42, 0x1732ccab.
                                                                                                                                                                                            level functions m
 pile your program 0xbabaefe5, 0xcc357360, 0xbf380d42, 0x1732ccab, 0x19f8c4e8, 0x78afc841, 0x3cbc1ddc, 0x63884fa3,
 cc hello-erase.c good
the following com
                                                                                                                                                                                           ne you found in s
                                                                                                                                                                                           you created in ste
 re "good" and "evil"
```

Se generaron los dos programas con ayuda de evilize.



Programa de Becas de Formación en Seguridad Informática Coordinación de Seguridad de la Información UNAM-CERT

```
Administración y seguridad en redes
re is based on Patr
                                           :~# echo "David Martin"
                                                                                                                                                            ation here.
                            David Martin
                                           :-# |
ge instructions:
ndows users:
                                                                         root@Kali: ~/Downloads/evilize-0.2
                                                                                                                                                               ↑ - □ × able fil
e", you must
                             Edit View Search Terminal Help
                     0xcd17e8ed, 0x38f2fd9d, 0xc15694e1,
0x05346d51, 0x20737fff, 0x8564a99f,
                                                                               0x507f8a34.
k the archive
                                                            0x8564a99f, 0x10a9ef77,
 zxf evilize-0.2
                     0x55bfbef3, 0x885b5ffe, 0x91d6cd90, 0xf3d867ef,
                     0x65f9154c, 0xbe2b8389, 0xcb7dcbf6, 0xcdellcaf, 0x960896cb, 0xlcb4ccf1, 0x56albd14, 0xe04cedd0,
evilize-0.2
                                        0xcc357360,
                     0xbabaefe5,
                                                            0xbf380d42, 0x17324cab,
reates the pro
                     0x19f8c4e8, 0x78afc841, 0xbcbc1ddc, 0x63884fa3,
e a C program };
                                                                                                                                                                            nain_go
evil(). See the
                     rootgKali:~/Downloads/evilize-0.2# ./evilize hola_vibora -c init.txt -g p_hola -e p_vibora
Writing 'good' file p_hola.
Writing 'evil' file p_vibora.
rootgKali:~/Downloads/evilize-0.2# ls -l
ile your progr
he following co
                      total 508
                                       1 dm dm 178 Oct 11 2011 AUTHORS
1 dm dm 172 Oct 11 2011 Changel
1 dm dm 17992 Oct 11 2011 COPYING
1 dm dm 581 Oct 11 2011 crib.h
1 root root 79872 Sep 30 17:21 evilize
1 dm dm 11832 Oct 11 2011 evilize
evilize hello-era
                                                                                 2011 AUTHORS
2011 ChangeLog
                                                                                                                                                                           step 4):
                                                                                2011 ChangeLo
2011 COPYING
2011 crib.h
e an MD5 collis - rw-rw----
md5coll 0x23d3e48
                                                             1032 Oct 11 2011 evilize
4848 Sep 30 17:21 evilize.c
461 Oct 11 2011 goode.co
6128 Sep 30
                       -rwxr-xr-x
this step can to
te a pair of goo
                                       1 root root 54848
1 dm dm 461
                                                                               2011 goodevil.c
17:21 goodevil.o
evilize hello-era
                       - rw-rw----
                                                            6128
 "good" and "ev
```

Se otorgaron los permisos correspondientes de ejecución y se probo la funcionalidad, así mismo se generaron los dos hashes MD5..... con coincidencia exacta.

```
uctions:
                                                                 root@Kali: ~/Downloads/evilize=0.2
sers
                                                                                                                                                                 must
                   Edit View Search Terminal Help
                    ali:~/Downloads/evilize-0.2# ls -l p_*
-r-- 1 root root 10560 Sep 30 19:14 p_hola
-r-- 1 root root 10560 Sep 30 19:14 p_vibora
ali:~/Downloads/evilize-0.2# chmod ugo+x p_*
chive
            cot@Kali:~/Downloads/evilize-0.2# ls -l p_*
rwxr-xr-x 1 root root 10560 Sep 30 19:14 p_hola
           -rwxr-xr-x 1 root root 10560 Sep 30 19:14 p_vibora
gram
                          :~/Downloads/evilize-0.2# ./p_hola
e the
                    mundo!
progr
                         :~/Downloads/evilize-0.2# ./p_vibora
          ya te atrapo la vibora!!!
Erasing hard drive...1Gb...2Gb... caiste!
ing co buendia.
                          :~/Downloads/evilize-0.2# md5sum p_hola
          c659bed21b3476f7baf46ba5c24f6dd5 p_hota

rootgKali:~/Downloads/evilize-0.2# md5sum p_vibora

c659bed21b3476f7baf46ba5c24f6dd5 p_vibora

rootgKali:~/Downloads/evilize-0.2# echo "listo , David Martin"
           listo , David Martin
                         :~/Downloads/evilize-0.2#
of goo
```



Programa de Becas de Formación en Seguridad Informática Coordinación de Seguridad de la Información UNAM-CERT Administración y seguridad en redes

## **BIbliografia**

Selinger, Peter. MD5 Collision. https://www.mscs.dal.ca/~selinger/md5collision/

Stevens, DIdier . Playing With Authenticode and MD5 Collisions. https://blog.didierstevens.com/2009/01/17/playing-with-authenticode-and-md5-collisions/