C++ Tricks 2.3 I386C

farseerfc.wordpress.com

2.3 I386C

espesp

espespespebpebpebp

```
void f()

{

int a=0; //aebp-4

char c=1; //cebp-8

}
```

```
push ebp ;ebp

mov ebp,esp ;ebp=esp

sub esp,8 ;esp-=8ac

mov dword ptr[ebp-4],0 ;a=0

mov byte ptr[ebp-8],1 ;c=1

add esp,8 ;esp+=8ac

mov esp,ebp ;esp=ebp

pop ebp ;ebp

ret ;
```

```
09992:c=1 <-esp

09996:a=0

10000:ebp <-ebp
```

10004:......

:poppushcallret

```
push ebp:

add esp,4

mov dword ptr[esp],ebp

pop ebp

mov ebp,dword ptr[esp]

sub esp,4

call fun_address

push eip

jmp fun_address

ret

add esp,4

jmp dword ptr[esp-4]

ret

ret 8

add esp,12

jmp dword ptr[esp-4]
```

```
void f()
{
int i,a[10];
for(i=0;i<=10;++i)a[i]=0;/An error occurs here!
}
```

C++“”

a[10]a[10]C++“”a[10]a i!

iaaI386aia[i]ia[i]i 0…………Kill……