

USMA SIGSAC

```
12     return 0;
13 }
14 int fib_seq(int s1, int s2, int n) {
15     int sequence[n];
16     sequence[0] = s1;
17     sequence[1] = s2;
18     for(int i = 2; i < n; i++) {
19         sequence[i] = sequence[i-1] + sequence[i-2];
20     }
21     return sequence[n-1];
22 }
23 int shmoocon(int one, int two, int three) {
24     int returnVar;
25     if(one==1) {
26         returnVar = two+three;
27     } else if(one==2) {
28         returnVar = two*three;
29     } else if(one==3) {
30         returnVar = fib_seq(two, three, 10);
31     } else returnVar = 0;
32     return returnVar;
33 }
34
```

Assembly code for the functions above:

```

12     mov     eax, [esp+0x10]
13     mov     DWORD PTR [esp+eax], 0
14     call    0x804835c <gets@plt>
15     mov     eax, 0x8048585
16     lea     edx, [esp+0x10]
17     mov     DWORD PTR [esp+0x4], edx
18     mov     DWORD PTR [esp], eax
19     call    0x804838c <printf@plt>
20     mov     eax, 0x0
21     leave
22     ret     ctx->a, ctx->b, ctx->c
23
24     jmp     DWORD PTR ds:0x80496a0
25     push    0x20a, ctx->b, ctx->c
26     jmp     0x804833c
27
28     mov     eax, 3
29     push    0x8, 5
30     jmp     0x804833c
31
32     jmp     DWORD PTR ds:0x80496a0
33     call    0x804838c
34     xchg    edx, eax
35     add     DWORD PTR [eax+ecx*1], 0x0

```

SIGSAC -- Agenda

1. Admin (Haxathon + CSAW)
2. Get VMs up and running
3. Use aircrack WEP cracking tutorial to crack WAP

SIGSAC

■ On the Horizon

■ Haxathon

- REGISTER HERE: <http://haxathon.com>

■ CSAW CTF

■ Buffer overflow lesson

■ Lock picking

SIGSAC – IRC

- Use your IRC client of choice to connect to:
 - irc.cyclonecobra.com channel #sigsac
 - alternate: irc.freenode.net #usmasigsac
- Benefits of IRC: you can ask for help and get immediate response from more experienced members.

SIGSAC – Virtual Machine

- Virtualbox installed, ubuntu (or backtrack) .iso downloaded.
- Might want to install guest additions to share files with VM.

SIGSAC – WEP Cracking

- WEP is extremely easy to crack... anyone with Google can do it.
- Breaking into secured Wifi networks without permission is illegal.

SIGSAC – WEP cracking

- http://www.aircrack-ng.org/doku.php?id=simple_wep_crack
(^^ blocked on DREN)
- Grab aircrack files from usmasigsac.com
 - <http://www.usmasigsac.com/files/lsn2/aircrack-deb.zip>
 - Tutorial and .deb file are included
- Connect to sigsac WEP network