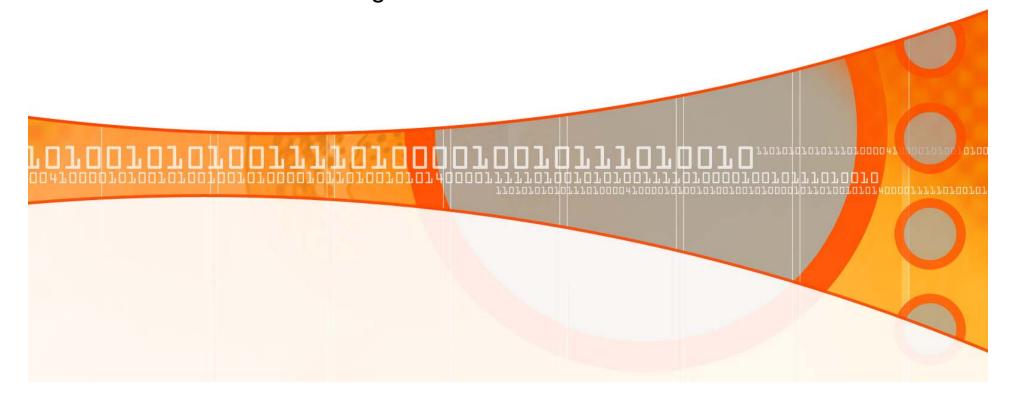


Reverse Engineering for fun and ... BoF it!

Pedram Amini and Chris Eagle



Introductions and Agenda

Pedram Amini

TippingPoint, a division of 3Com

Chris Eagle

- Associate Chair, Computer Science, Naval Postgraduate School
- RE has gotten a lot of attention in the past year
- The goal of this session is to present ideas and resources to foster an open discussion.
- What are the motivations for RE?
- Please introduce yourself before speaking

RE in the News 2005-Present

- Sony Rootkit debacle
 - Mark Russinovich (http://www.sysinternals.com/blog/)
- Microsoft WMF unofficial patch
 - Ilfak Guilfanov
- Blizzard World of Warcraft "rootkit"
 - Greg Hoglund
- Any other news?

RE Resources 2005-Present

- OpenRCE.org
- IDA SDK reference manual
 - Steve Micallef
 - http://www.binarypool.com/idapluginwriting/
- Ilfak Guilfanov's weblog
 - http://www.hexblog.com
- Books
 - Reversing: Secrets of Reversing
 - Disassembling Code: IDA Pro and SoftICE
 - Hacker Debugging Uncovered
 - Rootkits: Subverting the Windows Kernel
- What do you want to see?

RE Tools 2005-Present

- IDA Python
 - REML
- Visualization
 - Process Stalker
 - Sabre Bin Navi
 - IDA 5.0
- x86 Emu
- Collaborative
 - IDA Sync / Olly Sync
- Diffing
 - Sabre Bin Diff
 - IDA Compare

- Symbolic name
- Graph heuristics
- Recursive functions
- String references
- In/out degree
- Small prime product
- Shortest path
- MD5 / "smart" MD5
- Push + call
- Constants
- Stack frame size
- Spatial locality

IDA 5.0 Graphing



IDA 5.0 Graphing

```
; logging logic
                           do not log:
                                    esi, ds:std::operator<<<std::char traits<char>>(std::basic ostream<c
■ ■ □ # ∪
   loc 100A4415:
            edi, ds: imp_sprintf
    mov
            offset str InstanceName
    push
    push
            offset str ServiceType
    push
            offset str Domain 0
            edx, [ebp+var 194]
    lea
    push
            offset str TimestampARFlagsIf 24s 24sS; "Timestamp
                                                                    A/R Flags if %-24s %-24s "..
    push
    call
            edi ; __imp_sprintf
    push
    call
    add
            esp, 18h
            al, al
    test
            short loc 100A449B
    jz
                                          ; logging logic
                                 loc 100A449B:
                                  lea
                                          eax, [ebp+var 294]
                                  push
                                          eax
                                          sub 100A2110
                                  call
                                          eax, [ebp+arg 10]
                                  mov
                                  add
                                          esp,
                                  test
                                          eax, eax
```

RE Tools Future

- PyDBG
- RE-Sync
- x86 Emu +visualization?
- What road blocks have you hit?
- What tools would you like to see?



http://www.openrce.org/shmoocon

