Integrating DMA attacks in exploitation frameworks

Rory Breuk    Albert Spruyt

University of Amsterdam

February 7, 2012
Research Question:
How can DMA attacks be integrated into an exploitation framework?

Previous work
- FTWAutopwn
- libforensic1394
- Payloads

Why?
- Huge potential, but under utilized
- Widespread awareness is lacking
- Making it easy
- Different from buffer overflows
- Lots of possibilities
Local attacker

IEEE1394

Internet

Remote attacker

Target
DMA - protocol analysis

- FireWire
- eSATA
- USB - On The Go
- Thunderbolt
- PCMCIA
Exploitation frameworks

- Core Impact
- Metasploit Framework
- CANVAS
- Volatility
Metasploit concepts

- Exploits
- Payloads
- Sessions
Integration

- libforensic1394
- Inserting code
- Metasploit reverse shell
- Cleaning up
- FireWire data connection
- Runs in userspace
- Injectable
- Cache coherency
Payloads

What to patch

```assembly
.text:0805650A  mov     [esp+14h], eax
.text:0805650E  mov     eax, [edx+1Ch]
.text:08056511  mov     [esp+10h], eax
.text:08056515  mov     eax, [edx+24h]
.text:08056518  mov     dword ptr [esp+48], offset aPam_authentic  
.text:08056520  mov     dword ptr [esp+4], 80h
.text:08056528  mov     dword ptr [esp], 0
.text:0805652F  mov     [esp+6Ch], eax
.text:08056533  call    q_log
.text:08056538  mov     esi, [ebx+0Ch]
.text:0805653B  mov     eax, [esi+1Ch]
.text:0805653E  test    eax, eax
.text:08056540  jmp     short loc 8056560
.text:08056542  ; -----  
.text:08056546  mov     [esp+4], ebx
.text:0805654C  mov     dword ptr [esp], offset sub_8057370
.text:08056550  call    _q_idle_add
.text:08056552  add     esp, 24h
.text:08056555  xor     eax, eax
.text:08056557  pop     ebx
.text:08056558  pop     esi
```

Library call

Patch
Clean up - Act normal

Rory Breuk, Albert Spruyt (UvA)

Integrating DMA attacks

February 7, 2012 11 / 15
Metasploit demo

- Choose exploit and payload
- Change the settings for the modules
- Run exploit
  - Load payload into target
  - Depending on payload: achieve session between target and attacker
Mitigation

- Mitigation for end-users
- Don’t buy them
- Destroy them / glue them
- Disable them
- Deny physical access
Achievements:
- Show DMA vulnerabilities exist on different ports
- Port libforensic1394 bindings to Ruby
- Integrate FireWire exploit into Metasploit
- Clean payload execution
- Proof of concept FireWire data session
Questions?