EXHIBIT I
Volume 6

```
addi sp, sp, 0
ld r0, 0x10(s
mtlr r0
li r3, 0
blr
```

You have earned a trophy.

LV2 Code Execution

NO W^X in LV2

Any old exploit == code execution

Hypervisor allows unsigned code

It happily marks pages as executable and plays no role in enforcing that only trusted code runs

Results

- LV2 "GameOS" compromised
- LV1 Hypervisor NOT compromised
- Secure SPE NOT compromised

You have earned a trophy.
Piracy

- LV2 "GameOS" compromised
- LV1 Hypervisor NOT compromised
- Secure SPE NOT compromised
- Piracy

Fail Security Model

- The hypervisor does not enforce LV2 and game integrity
- You can just patch LV2 to run games from HDD

	Xbox	Wii	360	PS3
On-die bootROM	✓	✓	✓	✓
On-die key storage		✓	✓	
Public-key crypto	✓	✓	✓	✓
Chain of trust	✓		✓	✓
Per-console keys		✓	✓	✓
Signed executables	✓		✓	✓
Security coprocessor		✓		✓
Full media encryption and signing		✓		
Encrypted storage		✓		
Self-signed storage		✓		
Memory encryption/hashing			✓	
Hypervisor			✓	✓
User/kernelmode				✓
Anti-downgrade eFUSEs			✓	

BYPASSED

	Xbox	Wii	360	PS3
On-die bootROM	✓	✓	✓	✓
On-die key storage		✓	✓	
Public-key crypto	✓	✓	✓	✓
Chain of trust	✓		✓	✓
Per-console keys		✓	✓	✓
Signed executables	✓		✓	✓
Security coprocessor		✓		✓
Full media encryption and signing		✓		
Encrypted storage		✓		
Self-signed storage		✓		
Memory encryption/hashing			✓	
Hypervisor			✓	✓
User/kernelmode				✓
Anti-downgrade eFUSEs			✓	

BYPASSED

USELESS

	Xbox	Wii	360	PS3
On-die bootROM	✓	✓	✓	✓
On-die key storage		✓	✓	
Public-key crypto	✓	✓	✓	✓
Chain of trust	✓		✓	✓
Per-console keys		✓	✓	✓
Signed executables	✓		✓	✓
Security coprocessor		✓		✓
Full media encryption and signing		✓		
Encrypted storage		✓		
Self-signed storage		✓		
Memory encryption/hashing			✓	
Hypervisor			✓	✓
User/kernelmode				✓
Anti-downgrade eFUSEs			✓	

INEFFECTIVE

BYPASSED

USELESS

Downgrades

Downgrades

- Sony fixed the exploit

Downgrades

- Sony fixed the exploit
- Service mode triggered by USB "JIG"
  - HMAC authenticated, keys dumped