NetWatch

Joshua Wise
Jacob Potter
Who *really* runs code on your machine?

- Your program
- The kernel, when an interrupt happens
- ... and that’s it, right?
Is that all?

- What if you plug in a USB keyboard to Pebbles?
- Who controls the fans?
- Chipset bugfixes (what do those BIOS patches actually do?)
Introducing SMM

- Magic pin from the northbridge to the processor
- Acts like a completely separate CPU
- Hidden space in memory
- Introduced in 386SL, more widely in 486
Chain of events

- Something happens in northbridge
- Trap on certain devices, timer, I/O range
- SMI# signal goes low
- CPU acknowledges with SMI_ACT#
- “Uh oh...”, saves all state, vectors to...
That other memory...

- You can see all of RAM from ring 0, right?
- What about video RAM? What about the DRAM underneath?
- All controlled by northbridge - normally redirected, but can be changed on the fly
Chain of Events

• Starts executing code left behind by BIOS
• 16-bit flat “unreal mode”, cached segment selectors
• Saved state is in SMRAM segment too
• Can enter protected mode, turn on paging...
Blue Pill

- RSM instruction restores most state: CR0, CR3, segment descriptor caches, normal boring registers
- Undetectable, except for deliberate side effects, and a mysterious jump in the timers
Who’s afraid of the big, bad D_LCK?

- Northbridge registers also give access to SMRAM in “normal” mode
- Lets BIOS put things there in the first place
- One-way lockout bit to stop people like us
- SMM makes a great place for a rootkit
- But it’s not set in older machines
What are we doing?

- Introducing NetWatch
- What can you do with a server that won’t boot enough to give you SSH?
- Expensive network KVM?
- Drive over with a keyboard?
- We can control anything with SMM...
How hard can it be?

- Get code into SMM
- Access video RAM and registers, network card, keyboard, mouse...
- And plenty of glue
Components

- SMM loader: runs from GRUB before kernel
- I/O traps, network card interception
- TCP/IP: lwIP
- VNC?
How much code?

- SMM loader: 200 - 300 C, 50-60 asm
- I/O traps: 400 - 600 C
- TCP/IP: lwIP: 10k of lwIP, plus 100 - 200 C of glue
- VNC: 200 - 400 C
Current Status

• Running in SMM, trapping some I/O

• Can reboot a running Linux/Pebbles system on certain key presses

• Works “concurrently” with any running kernel

• Breaks ACPI
http://netwatchdev.blogspot.com/