The Hidden Nemesis: Backdooring Embedded Controllers

Ralf-Philipp Weinmann
University of Luxembourg
ralf-philipp.weinmann@uni.lu
Targets.
Targets.
You can be one, too.
Assume I briefly have physical access your laptop.
#FAIL for you, I know.
Your laptop is reinstalled/reimaged frequently.
You are excellent at forensics.
You can disassemble and reassemble your laptop blindfolded and clean it like your M-16.
You have written backdoors/rootkits yourself.
How would I backdoor your box?
Backdoors in laptops

- State of the art:
  - Hardware (e.g. keylogger: modified keyboard)
  - Software (usually hooks into operating system's keyboard handler)
  - BIOS (see CORE's talk), ACPI (Heasman)
- What about firmware of other devices?
  - Network card? Graphics card? HDD? AMT?
- Anything else?
That's what this talk is about!
Embedded controller

- Microcontroller in (almost?) every PC laptop
  - MacBooks have SMC instead
    - keyboard is connected through USB
- 8- or 16-bit MCU, Reneses widespread in ThinkPads
- Controls sensors and actuators:
  - temperature, battery, fans, brightness, LEDs
- Also responsible for hotkeys (e.g. enable VGA out, brightness control etc.)
- Hence: needs access to stream of key presses
MCUs rocking it old school...
MCUs rocking it old school...

(EP)ROM inside.
Some common ECs

- ENE: KB8910, KB926C/D, KB3310, KB3700 etc. as well as SMSC
- 8051 based, 8-bit MCU
- ITE (usually includes Super I/O controller): IT8500, IT8502E, IT8516, IT8301 etc.
- 8052 core, 8-bit MCU
- Nuvoton
  - CR16 core and others 8051 core
- Fujitsu: MB90378, 16-bit core
ThinkPad ECs

- Renases H8S, clocked at 10Mhz
- Powered when laptop has power (laptop may be turned off)
- BIOS and EC code can be flashed over LAN (disable this BIOS option if you own a ThinkPad!)
- Prior work on reversing them (benign, for fixing bugs)
- IDA Pro Advanced has support for the H8S
Prior work

- Commented disassemblies available for T43
- Pins/data lines identified
  - keyboard scan matrix
  - LEDs/ThinkLight
  - fan control
- Some patches available to fix annoyances
Source-equivalent!

http://ec.gnost.info/ec-18s.7z

; Source Equivalent for ThinkPad Embedded Controller Firmware

; H8S/2161BV Pin Assignments
; 32..25 PE -> keyboard scan matrix outputs
; 50..43 PF -> keyboard scan matrix outputs
; 58..51 PG <- keyboard scan matrix inputs
;  108 P13 -> BJT -> ThinkLight LED
;    3 P44 -> BJT -> IGFET -> fan motor
;    80 P62 <- BJT <- fan tachometer signal
 [...] 
; Type 1R: T40/p; T41/p; T42/p; R50/p; R51 1829..1831, 1836
 [...] 
; Type 1Y: T43/p 2668..2669, 0x2678..2679, 0x2686..2687
 [...] 
; Type 70: T43 1871..1876; R52 0x1858..1863, 0x1958
 [...] 
; Type 76: R52 1846..1850, 1870
 [...] 
; Type 1V: R50e, R51 2883, 0x2887..2889, 0x2894..2895 ; not supported
THE BACK DOOR
The PROMIS backdoor folklore

- Promis often was sold together with a computer.
- Anyone remember Inslaw?
- Inventor of Prosecutor’s Management Information System, a people-tracking software.
- Lots of legal fights about this software.
- Pirated, backdoored versions allegedly sold by CIA and/or Mossad to foreign governments.
More on PROMIS

- PROMIS and computer (e.g., a Prime) were sold as bundle
- Hardware of computer was backdoored, allegedly contained two chips
  - storage chip ("Elbit") [using "ambient electricity"]
  - communication chip, using spread-spectrum modulation to periodically transmit entire contents of database and/or keystroke buffer ["Petrie” chip]
- Let’s do it without the additional hardware!
Backdoor Capabilities

- For ThinkPads (only tested on X60s at the moment)
- Can record and exfiltrate keystroke data
- Assuming compression rate of 5:1 and 64KBytes scratch space → 300k keystrokes in ring buffer
- Data exfiltration
  - Can communicate with host CPU through ACPI or temperature readings
  - Get fancy: Modulate LEDs (Blinkenlights!) for optical and EM modulation!
Alternatives: JitterBugs

- Idea and first PoC by Shah, Molina and Blaze [Usenix Security 2006]
- Covert timing channel to leak key strokes
- PoC is bump-in-the-wire hardware implementation
- Firmware approach already suggested by authors
- Assumes bursted keyboard activity
- Uses inter-packet delays for a 1-bit channel
Defense

- EC firmware: not write-only, can dump it as well
- Build repository of known good versions and publish fingerprints (SHA-256)
- Ongoing project: http://coderpunks.org/ecdumper
- First release will be for ThinkPads only
- Contributions (for other models) welcome!
Outlook

- Want to cover more vendors/models
- Look into other devices with reflashable firmware:
  - BIOS/ACPI yesterday, ECs now, vPro/AMT next?
- Defense:
  - Build tools to fingerprint more laptop firmware
  - Make sure firmware is signed & verified
- Fundamental discussion on trust placed in firmware necessary