Low cost radio wave attacks on modern platforms

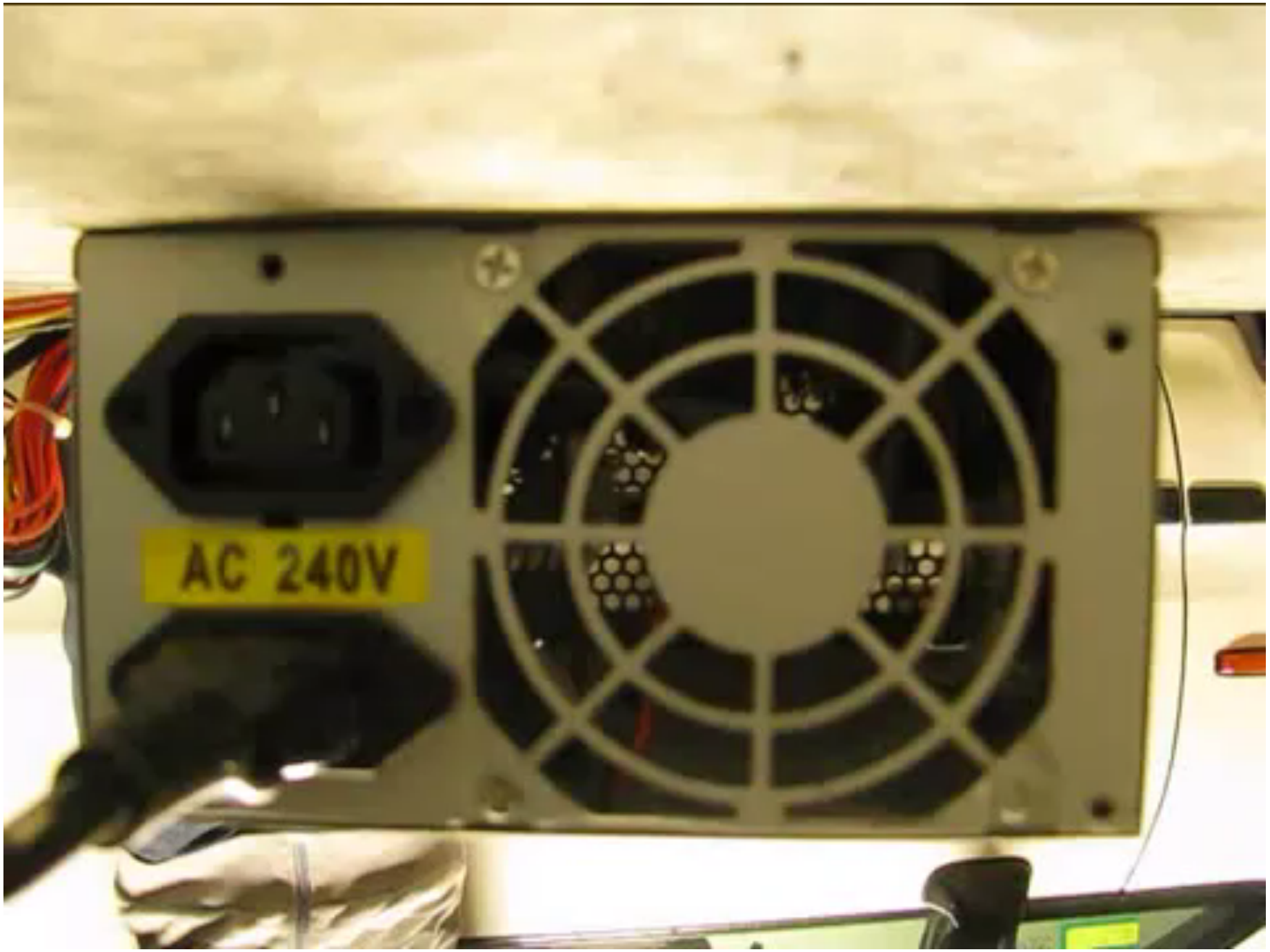
Mickey Shkatov

Maggie Jauregui

Intros

> Maggie Jauregui @MagsJauregui
> Mickey Shkatov @HackingThings

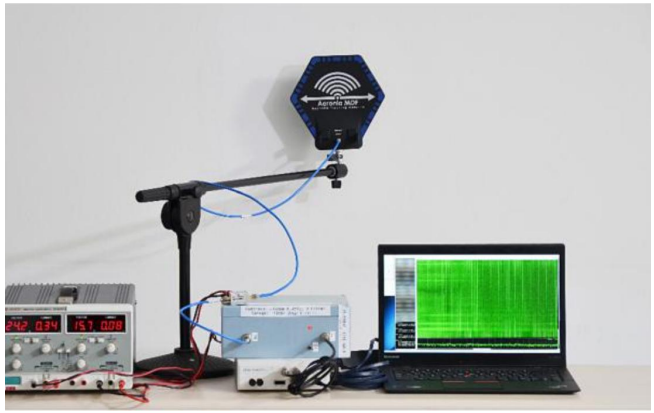
Backstory - DC22


AC 240V

“It works, I don’t know why”

- Hackers everywhere

EMI Previous work

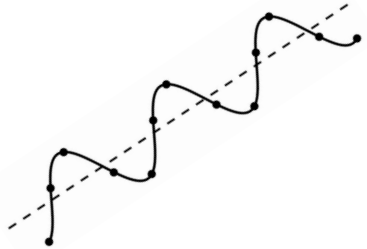


- Mainly passive...
  - Sniffing crypto keys across walls or performing side channel attacks

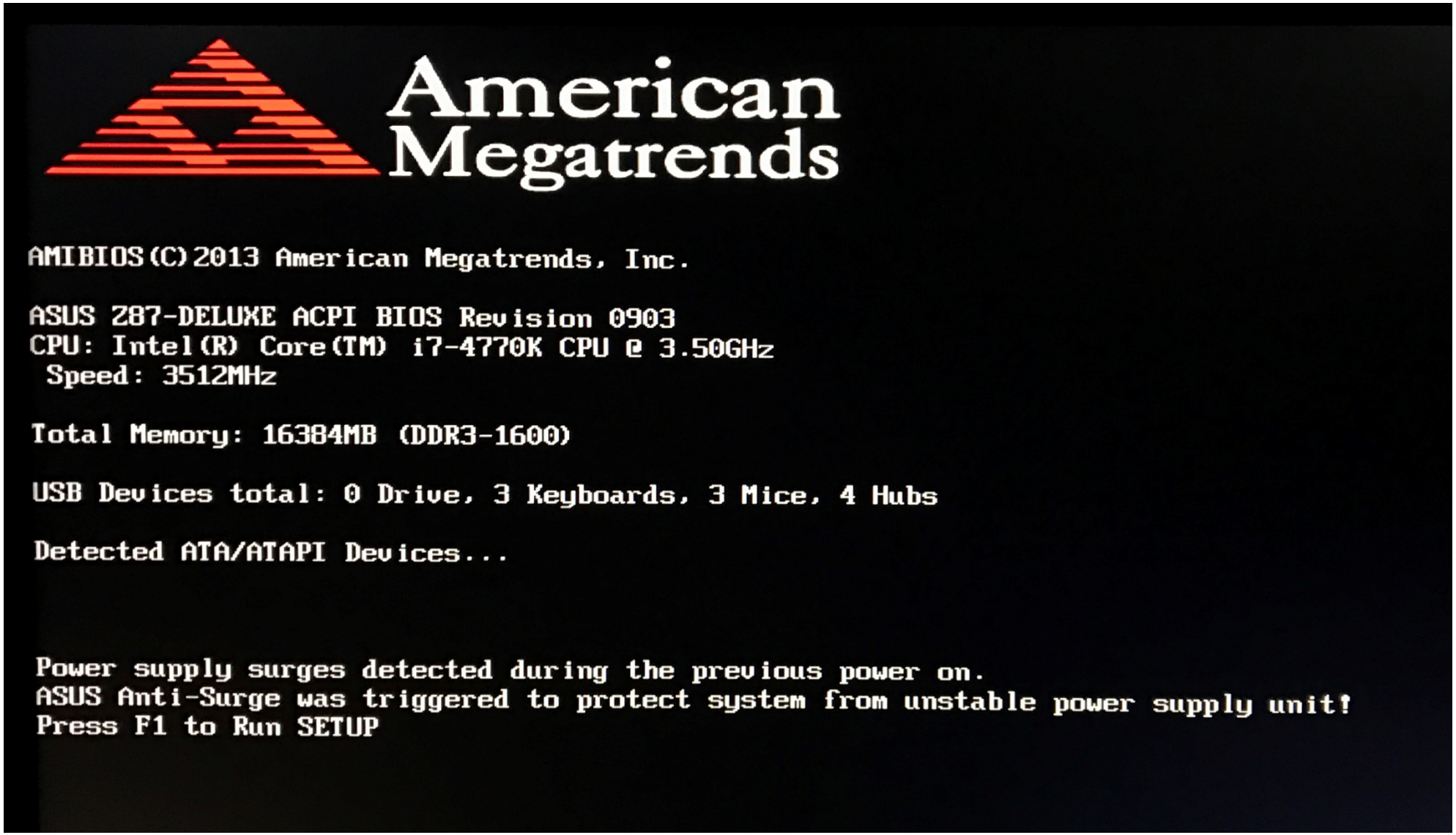
    https://motherboard.vice.com/en_us/article/how-white-hat-hackers-stole-crypto-keys-from-an-offline-laptop-in-another-room
  - FM Signals and Cell Phones Can be Used to Steal Data

    https://aabgu.org/fm-signals-cell-phones-can-used-steal-data/
  - Lunchbox Glitching for fun & no profit
    https://depletionmode.com/2015/11/05/lunchbox-glitching-for-fun-non-profit/

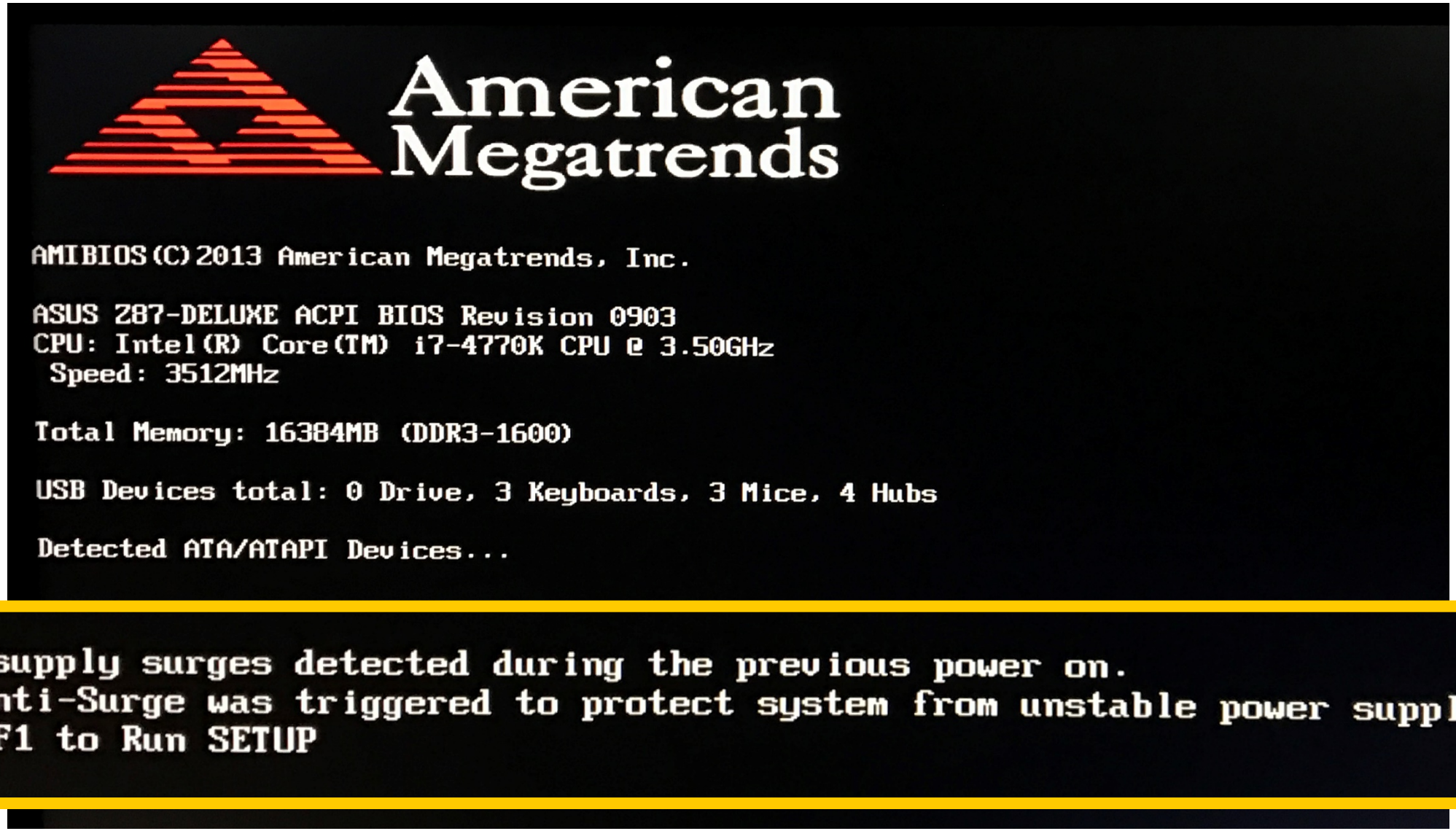
Demos



i. Power Surge

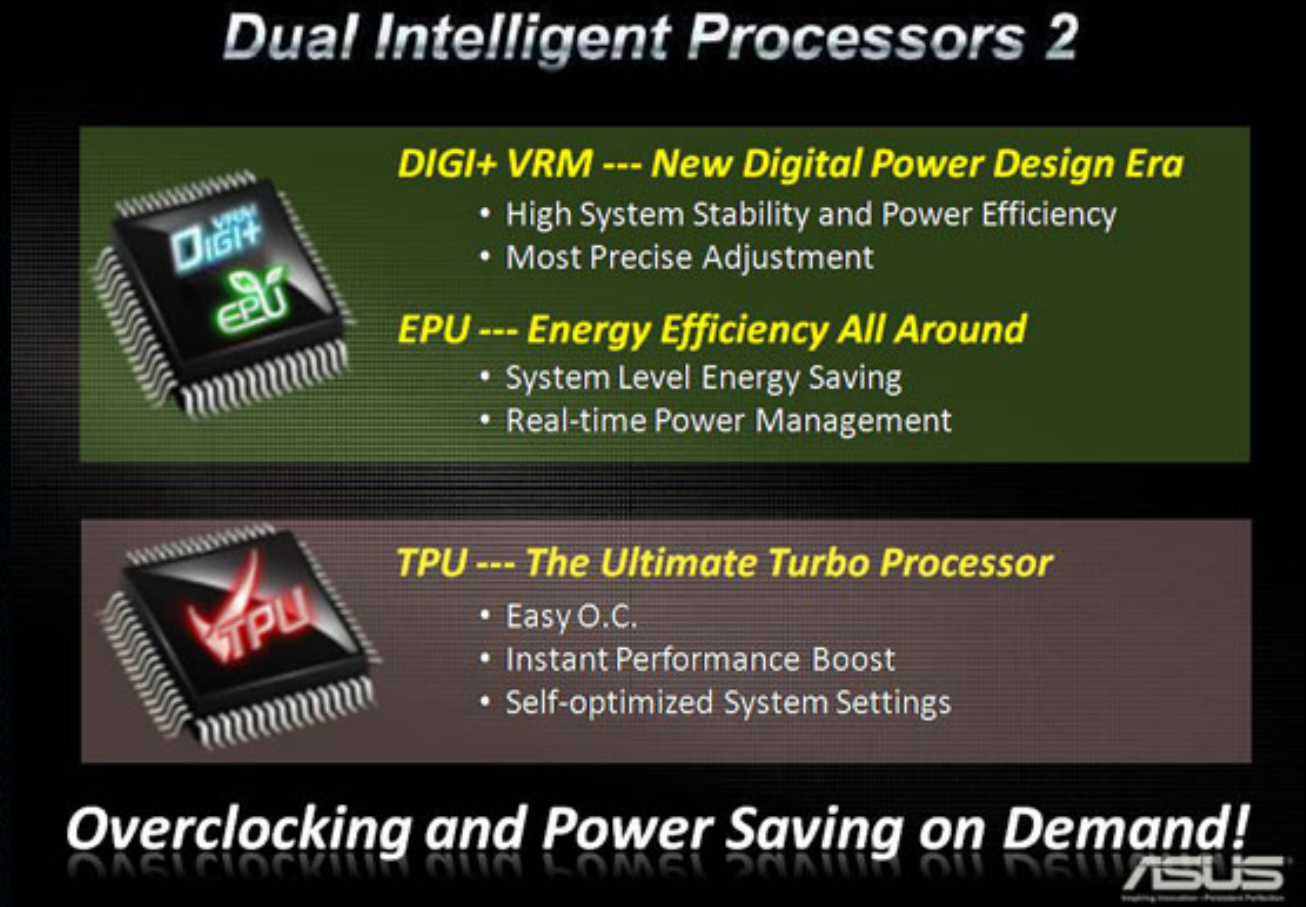


Power Surge


American Megatrends
AMIBIOS(C)2013 American Megatrends, Inc.
ASUS Z87-DELUXE ACPI BIOS Revision 0903
CPU: Intel(R) Core(TM) i7-4770K CPU @ 3.50GHz
Speed: 3512MHz
Total Memory: 16384MB (DDR3-1600)
USB Devices total: 0 Drive, 3 Keyboards, 3 Mice, 4 Hubs
Detected ATA/ATAPI Devices...
Power supply surges detected during the previous power on.
ASUS Anti-Surge was triggered to protect system from unstable power supply unit!
Press F1 to Run SETUP

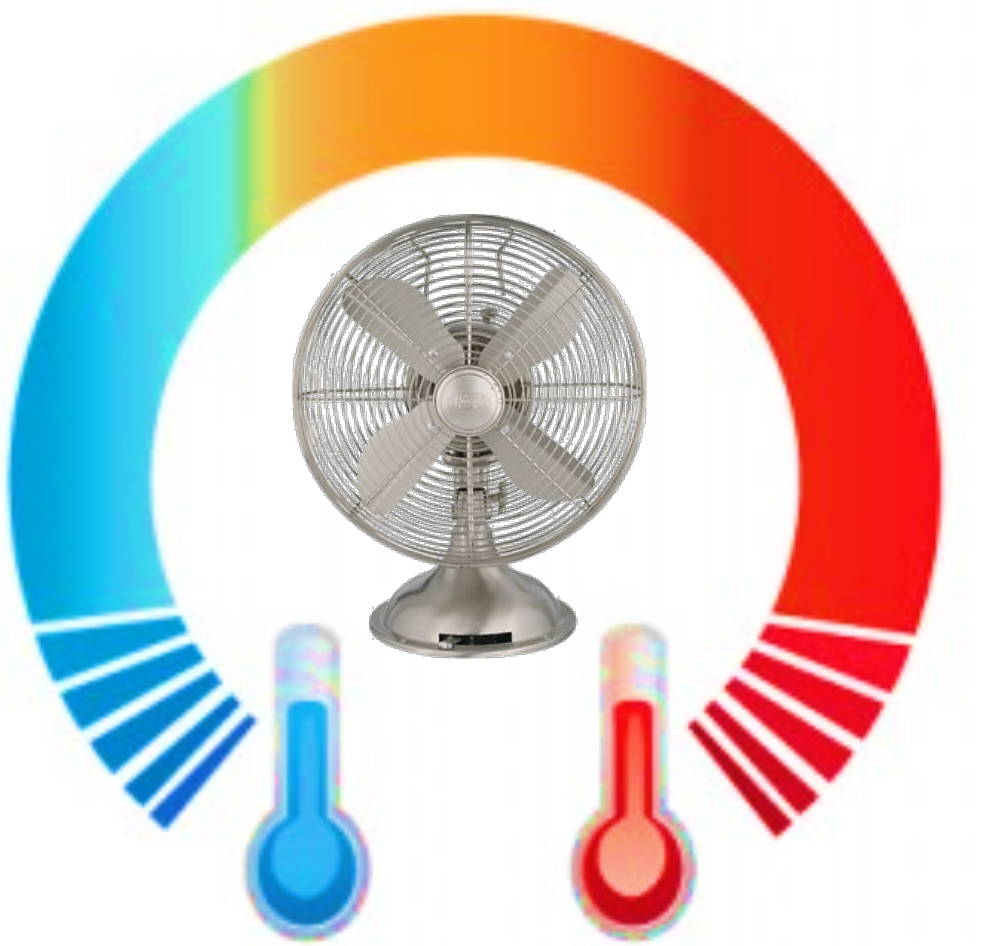
Power Surge

> ASUS DIGI+ VRM EPU
> ASUS TPU



ii. Sensor corruption/fan speed

> Tmp sensors [OS vs BIOS]
>> > CPU
>> > System
> Fan speed
> CPU core voltage



In case you missed it…

Sensor corruption/fan speed

Sensor corruption/fan speed

Fintek

Feature Integration Technology Inc.

F71889E

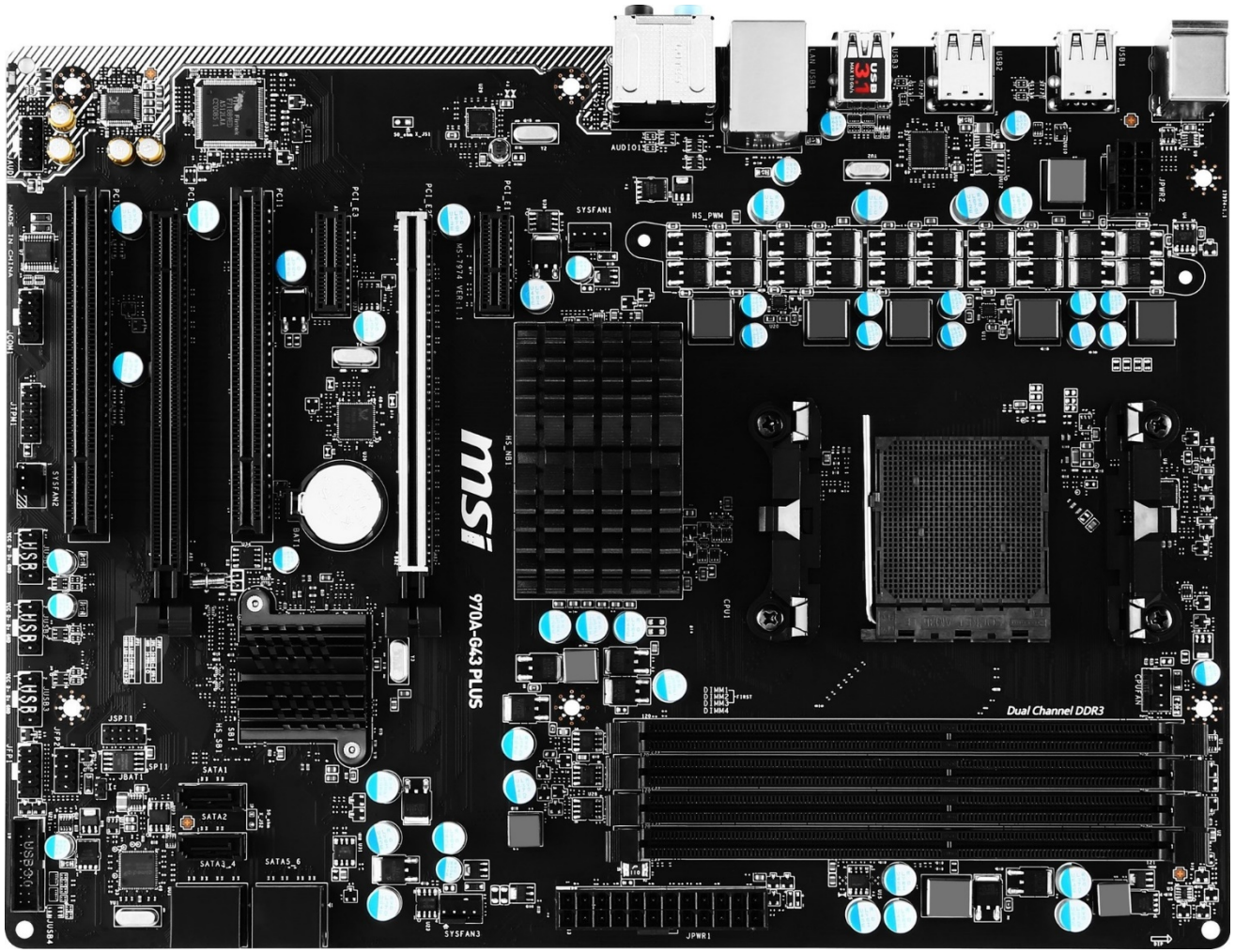
1. General Description

The F71889E which is the featured IO chip for new generational PC system is equipped with one IEEE 1284 parallel port, two UART ports, KBC, 80-Port, SIR, and VID controller. The F71889E integrated with hardware monitor, 9 sets of voltage sensor, 3 sets of creative auto-controlling fans and 3 temperature sensor pins for the accurate dual current type temp. measurement for CPU thermal diode or external transistors 2N3906.

Sensor corruption

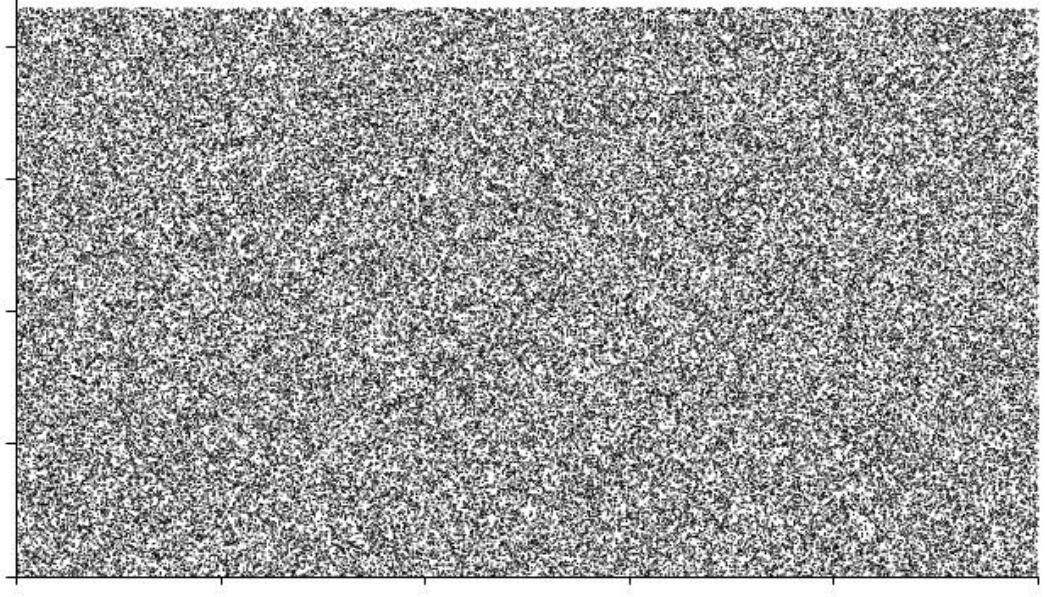
> Back-up video

iii. Powering motherboard components



Potential impact

</pun intended>



> RNG?
> Fire Hazard
> Memory corruption
> PDOS: Fry CPU/components
> Targeted glitching attacks
> Control over capacitance input systems <wip>
> Remote attacks via KVM
> HW Implants

Mitigations

- FC all the things!
  - Non-windowed chassis
- EM shielding. Don’t cheap out on...
  - Power supplies
  - Mother boards - Voltage regulators
- Built-in fault tolerance


Q&A

Back up…

iv. Bonus demo: BSOD