

Krótką historia o debugowaniu laptopa, który nie budził się z uśpienia

15.05.2019, Warsaw C++ Users' Group
Michał “Redford” Kowalczyk

O mnie

- Wicekapitan @ [Dragon Sector](#) CTF team
- Researcher @ [Invisible Things Lab](#)
- Inżynieria wsteczna, IT sec, kryptografia
- Współautor “Praktycznej Inżynierii Wstecznej”
- [dodane po prelekcji] Inna moja prezentacja, na podobny temat:
<https://www.youtube.com/watch?v=FpaBnJO9a0w>



Intro

- Znajomemu nie działa suspend w laptopie
- Usypia się poprawnie, ale hard reset przy próbie obudzenia
- Thinkpad x230, Qubes OS (z Xenem jako hypervisorem)

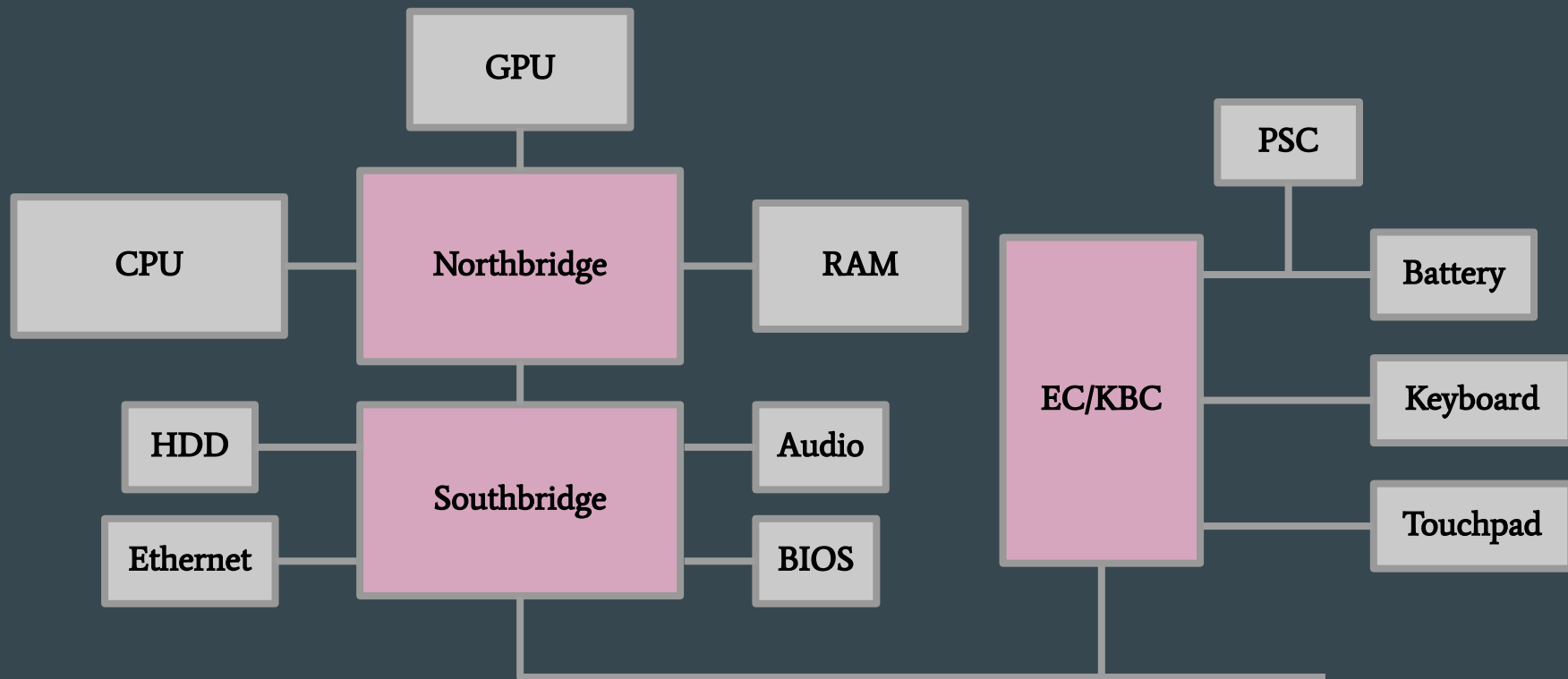
Standardowe sprawdzenia

- Update BIOS-u, firmware'u i sterowników
- Reset BIOS-u do ustawień fabrycznych
- Przełożenie dysku do innego Thinkpada x230
- Zmiana BIOS-u na coreboota
- Zmiana OS-a na inny

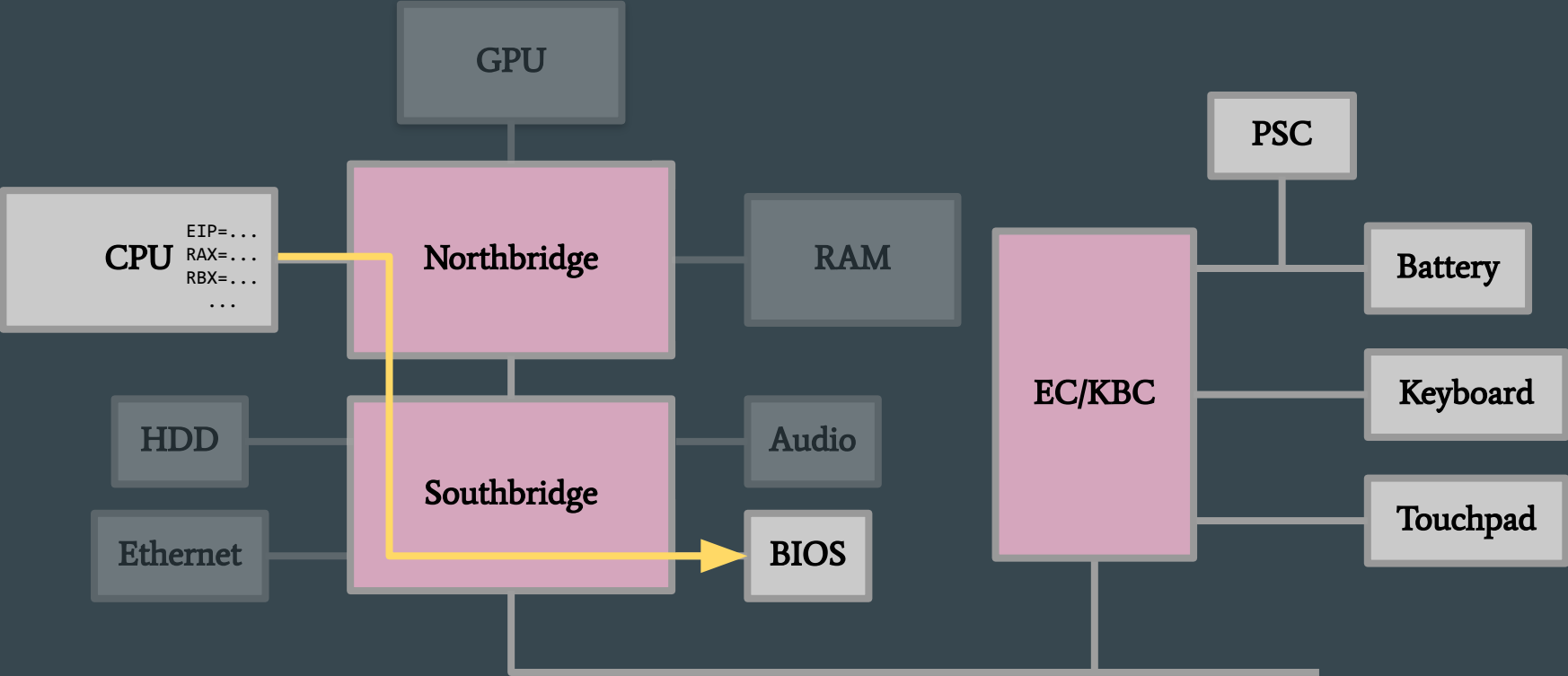
Nie widać żadnej oczywistej przyczyny → pora na debugowanie!

Ale najpierw, jak to wszystko działa?

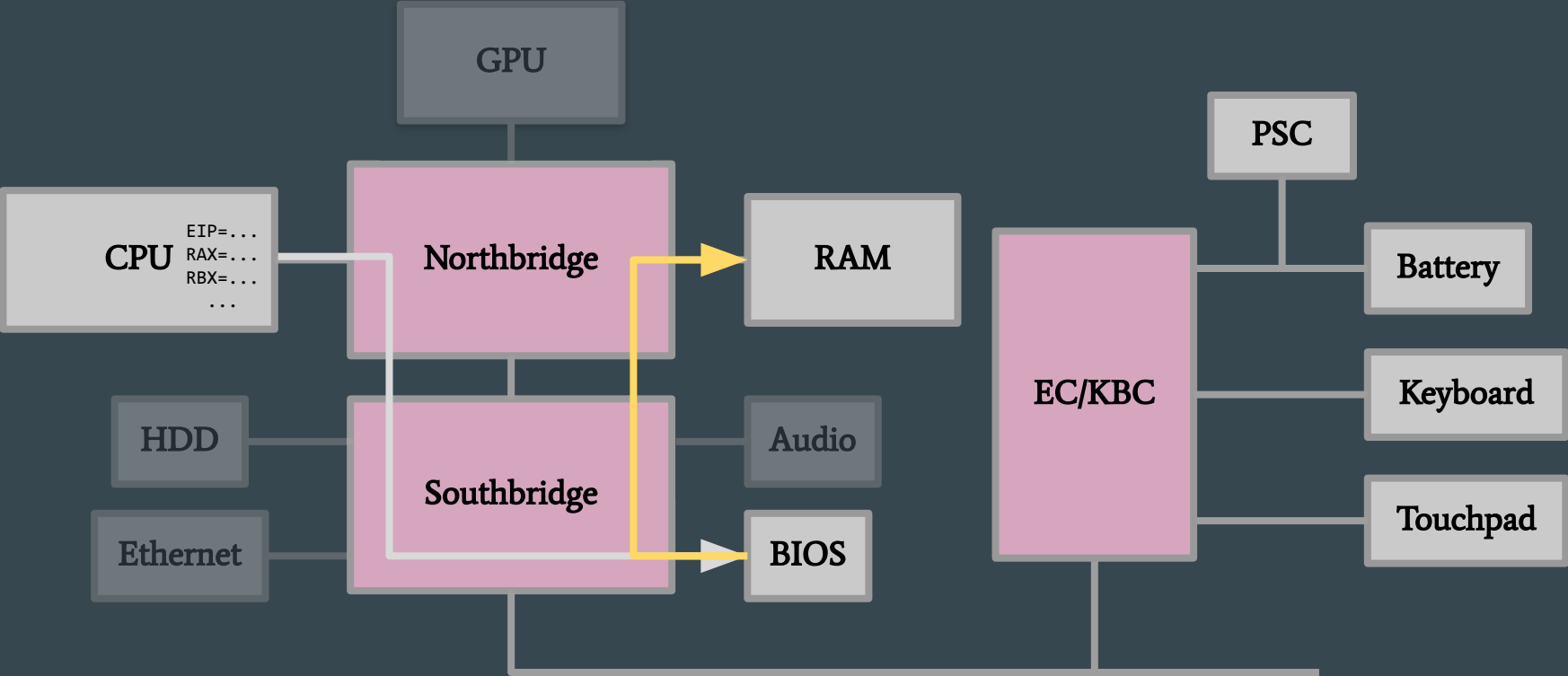
Jak działa komputer: BIOS, ACPI, OS...



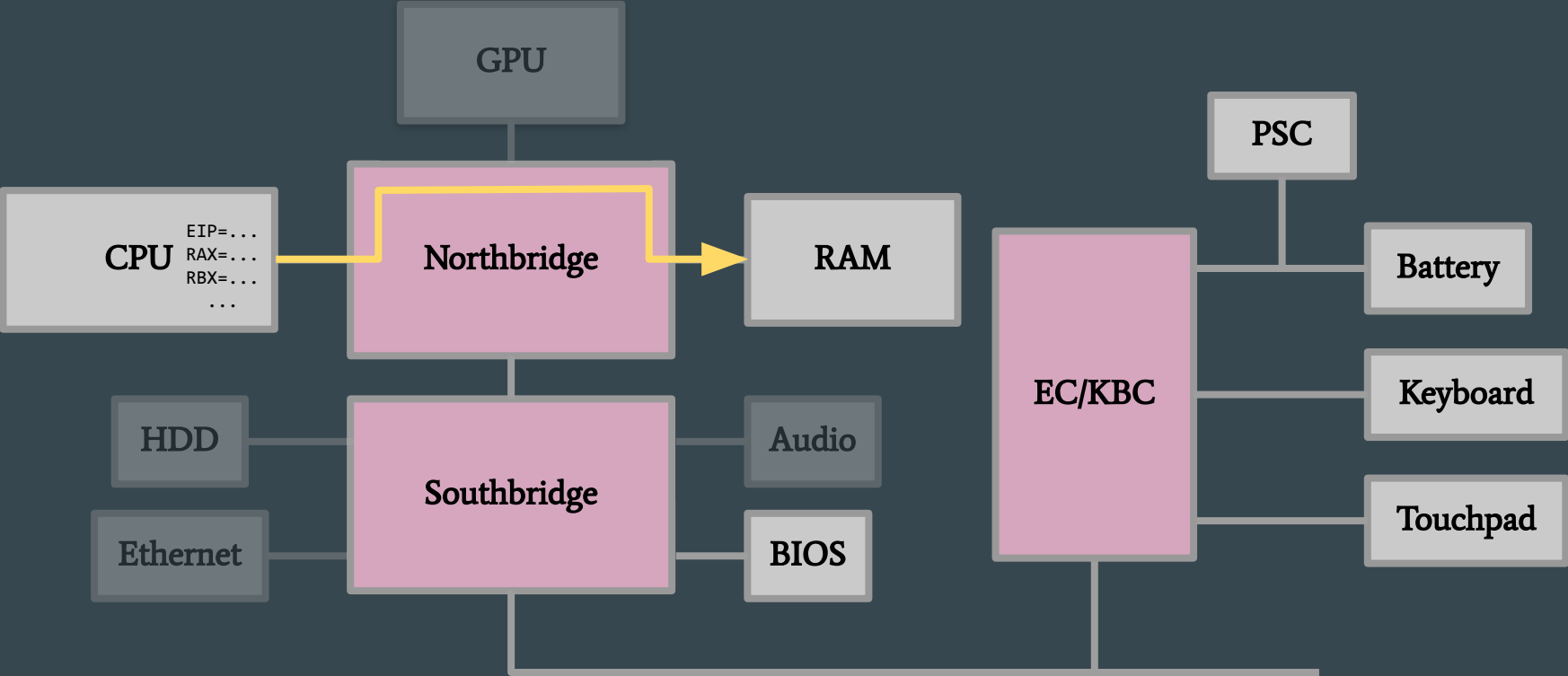
Boot



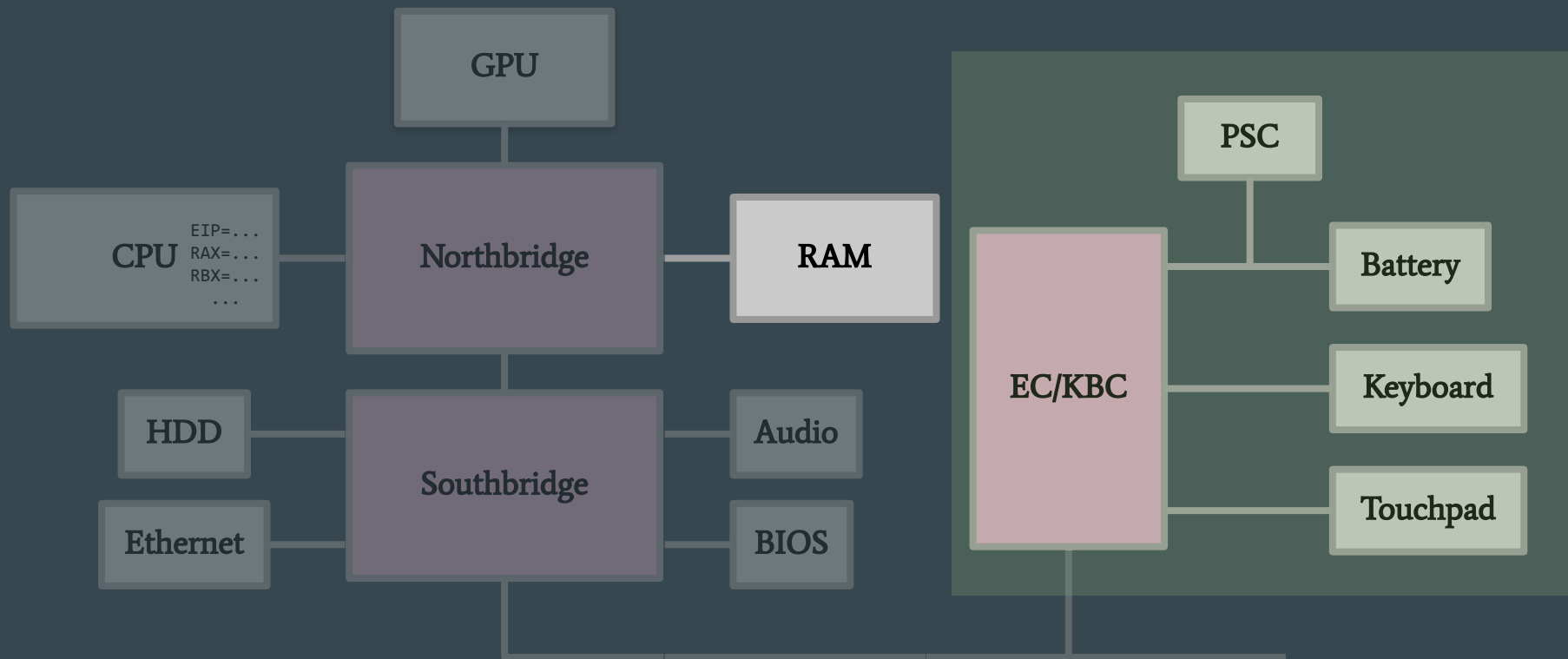
Boot



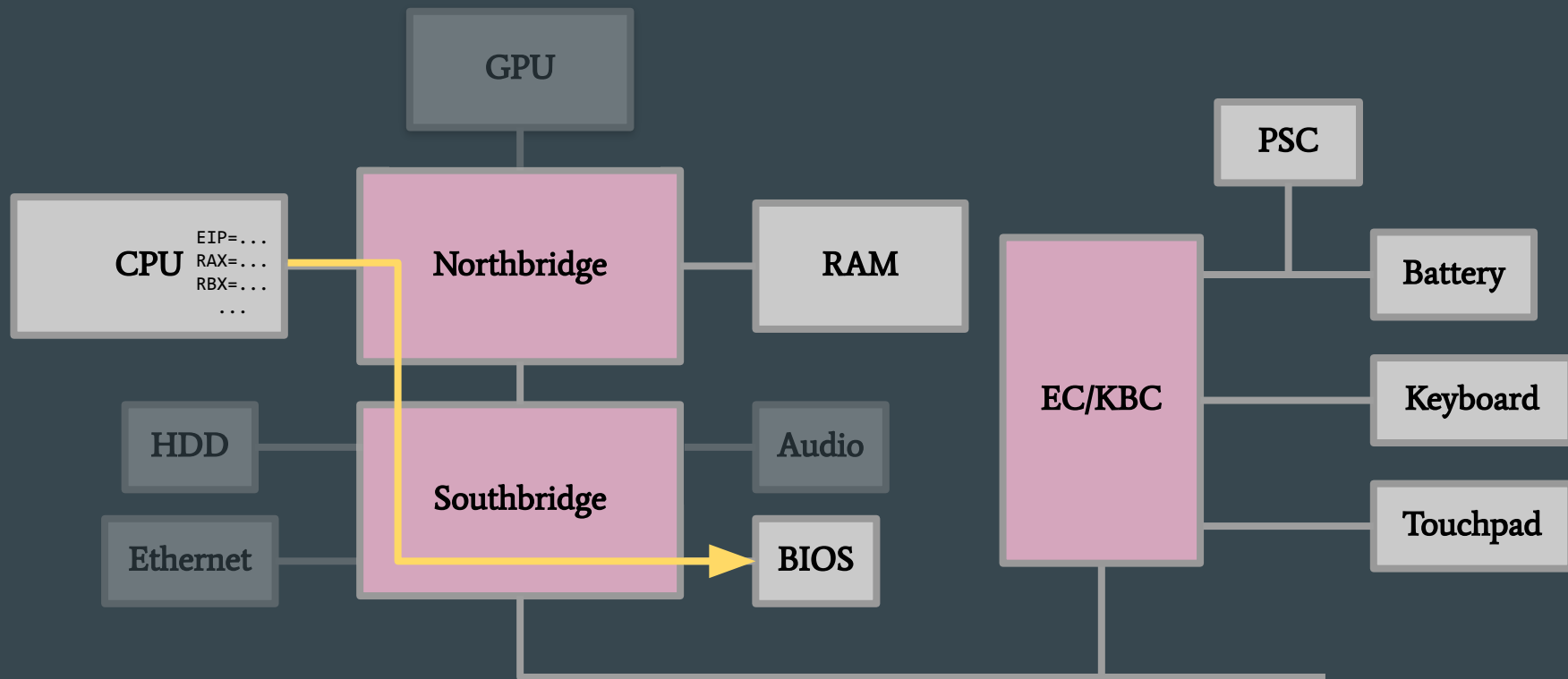
Boot



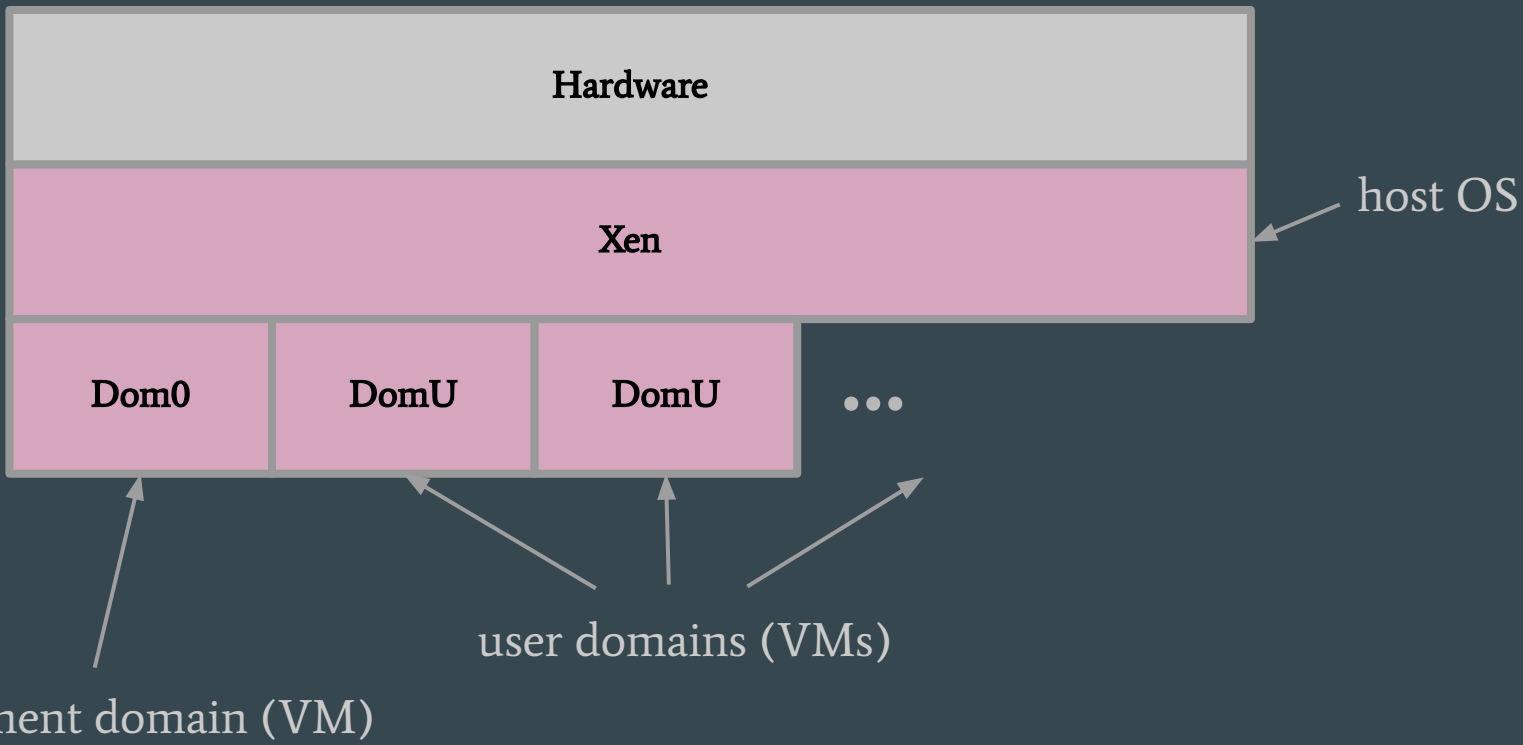
Przejsie w S3



Budzenie z S3



Qubes OS / Xen



Debugowanie

Sposoby na debugowanie

- Ekran - wyłączony/gpu wyłączone
- Serial port - nie mamy stacji dokującej
- `while (1) {}`
- RTC timer


pm_trace

- Ficzer Linuxa do debugowania ACPI

```
static int device_resume_noirq(struct device *dev, pm_message_t state, bool async)
{
    pm_callback_t callback;
    const char *info;
    bool skip_resume;
    int error = 0;

    TRACE_DEVICE(dev);
    TRACE_RESUME(0);

    if (dev->power.syscore || dev->power.direct_complete)
        goto Out;
}
```



pm_trace

- w Dom0:
echo 1 > /sys/power/pm_trace
- suspend → resume → auto reboot → dmesg:
Magic number: 0:848:178
hash matches
[snip]/linux-4.14.74/drivers/base/power/main.c:1143

pm_trace

- w Dom0:

```
echo 1 > /sys/power/pm_trace
```

- suspend → resume → auto reboot → dmesg:

```
Magic number: 0:848:178
```

```
hash matches
```

```
[snip]/linux-4.14.74/drivers/base/power/main.c:1143
```

- Czyli:

```
Complete:
```

```
    complete_all(&dev->power.completion);  
    TRACE_SUSPEND(error);  
    return error;
```

- Suspend się powiodł, ale do resume w ogóle nie dotarło

pm_trace w Xenie?

- Nie ma, ale...
- ...przeportowanie z Linuxa do Xena okazało się dość proste
- Setup: netboot przez PXELINUX

Dokąd dociera wykonanie?

arch/x86/boot/wakeup.S#L152:

```
    movl    $MSR_EFER,%ecx
    rdmsr
    btsl    $_EFER_LME,%eax /* Long Mode      */
    btsl    $_EFER_SCE,%eax /* SYSCALL/SYSRET */
    btl     $20,%edi       /* No Execute?    */
    jnc     1f
    btsl    $_EFER_NX,%eax /* No Execute     */
1:    wrmsr
```

NX?

- Niewłaczanie NX naprawia problem
- Ale dlaczego NX nie daje się włączyć?

NX

Intel SDM, Volume 3:

If the execute-disable capability is not available, a write to set IA32_EFER.NXE produces a #GP exception.

Ale procesor w tym laptopie wspiera NX...

NX

IA32_MISC_ENABLE MSR:

34	<p>XD Bit Disable (R/w)</p> <p>When set to 1, the Execute Disable Bit feature (XD Bit) is disabled and the XD Bit extended feature flag will be clear (CPUID.80000001H: EDX[20]=0).</p> <p>When set to a 0 (default), the Execute Disable Bit feature (if available) allows the OS to enable PAE paging and take advantage of data only pages.</p> <p>BIOS must not alter the contents of this bit location, if XD bit is not supported. Writing this bit to 1 when the XD Bit extended feature flag is set to 0 may generate a #GP exception.</p>
----	--

BIOS!

- BIOS na Thinkpadach x230 domyślnie ma **wyłączony** NX
- Xen przy starcie komputera **nadpisuje** wyłączenie NX i z powrotem go włącza (najpierw w IA32_MISC_ENABLE a potem w EFER.NXE)
- Ale przy resume robi tylko to drugie

Naprawa

- Zmiana ustawień BIOS-u naprawia problem
- Patch do Xena też nie zaszkodzi

Pytania?

Email: redford@dragonsector.pl

Twitter: [@dsredford](https://twitter.com/dsredford)

IRC: Redford @ freenode.net

