

Patrik Veselík
Muzeum počítačů o.s.

SECURITY HARDWARE

OBSAH

- [000] Procesory
- [001] Urychlovače výpočetního výkonu
- [010] Mainframe
- [011] Šifrovací doplňky
- [100] Pevné disky
- [101] Streamery a jejich média
- [110] Likvidace datových médií
- [111] Bezpečnost bez šifrování

Jak chránit data?

Š

I

F

R

O

V

A

T

!

Jak chránit data?

Softwarová cesta je...

. . . p o m a l á . .

pojdme to **zrychlit!**

[000] Procesory

- [000] Procesory
- [001] Urychlovače výpočetního výkonu
- [010] Mainframe
- [011] Šifrovací doplňky
- [100] Pevné disky
- [101] Streamery a jejich média
- [110] Likvidace datových médií
- [111] Bezpečnost bez šifrování

[ooo] Procesory: IA-32

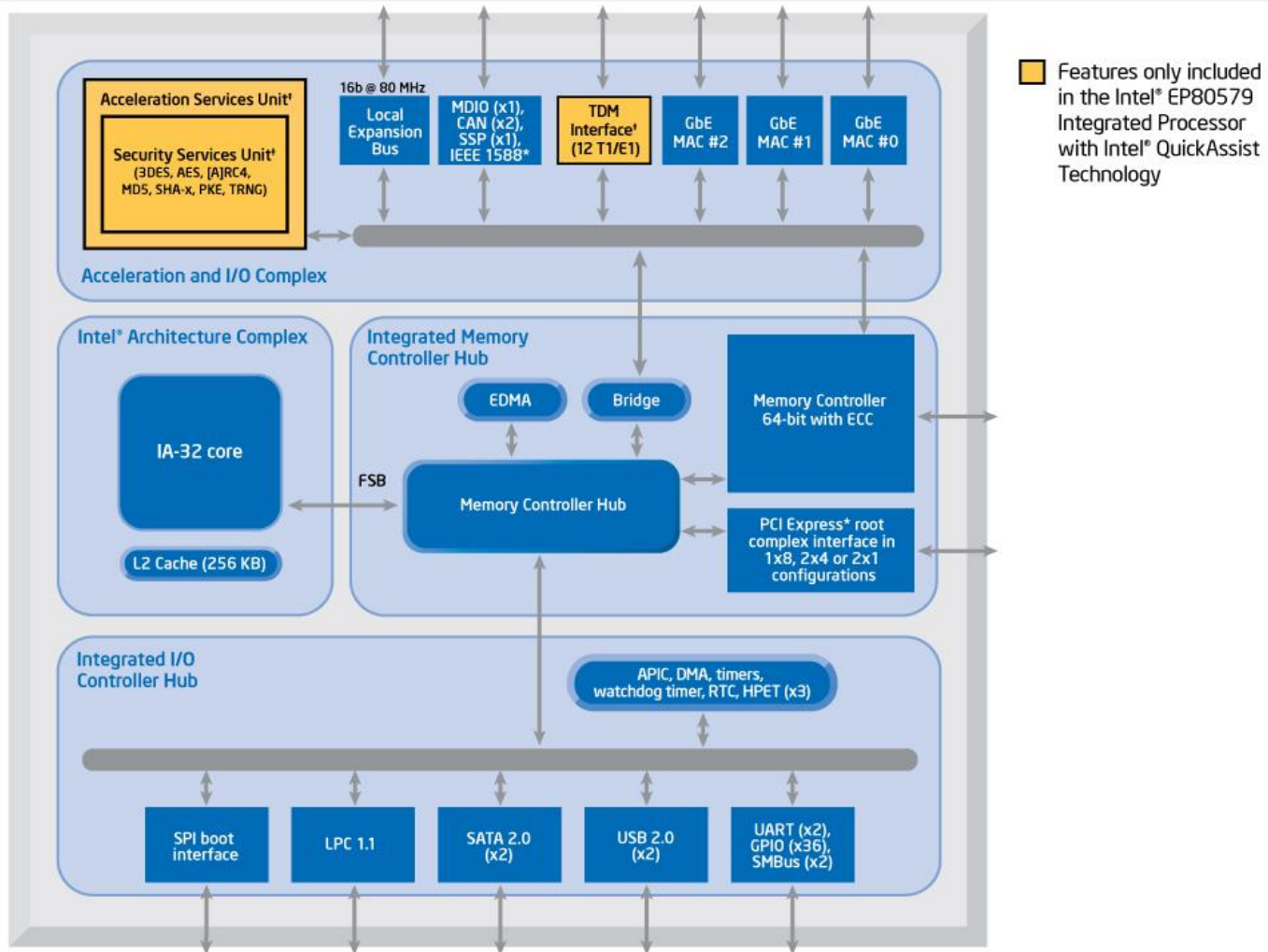
IA-32 rodina – kdo z nás ji neměl v počítači?
(Duron/Athlon *.* , Celeron/Pentium *.* apod.)

Drtivá většina procesorů IA-32 neumí šifrovat

Výjimkami jsou:

- AMD Geode LX
- Intel EP80579 with Intel QuickAssist Techno.
- VIA C3, VIA C7 (a průmyslové obdoby)

[ooo] Intel EP80579 with QAT



Block Diagram for the Intel EP80579 Integrated Processor and Intel EP80579 Integrated Processor with Intel QuickAssist Technology

[ooo] Procesory: „x64“

Rodina „x64“ – kdo z nás ji teď nemá v počítači?
(Athlon 64/Phenom *.* , *.Celeron/Core *.*)

Drtivá většina procesorů „x64“ neumí šifrovat

Výjimkami jsou:

- VIA Nano (a průmyslové obdoby)

...toť vše, přátelé!

[ooo] Procesory: „x64“

Rodina „x64“ se rozšíří o příkazovou sadu iAVX (SIMD jako MMX/SSE*.*/3DNow!/Altivec...)

Připravují se šifrovací instrukce (v rámci AVX):

AES-NI (6 příkazů pro AES_{128/192/256})

PCLMULQDQ (zrychlí eliptické křivky)

[ooo] Procesory: SPARC

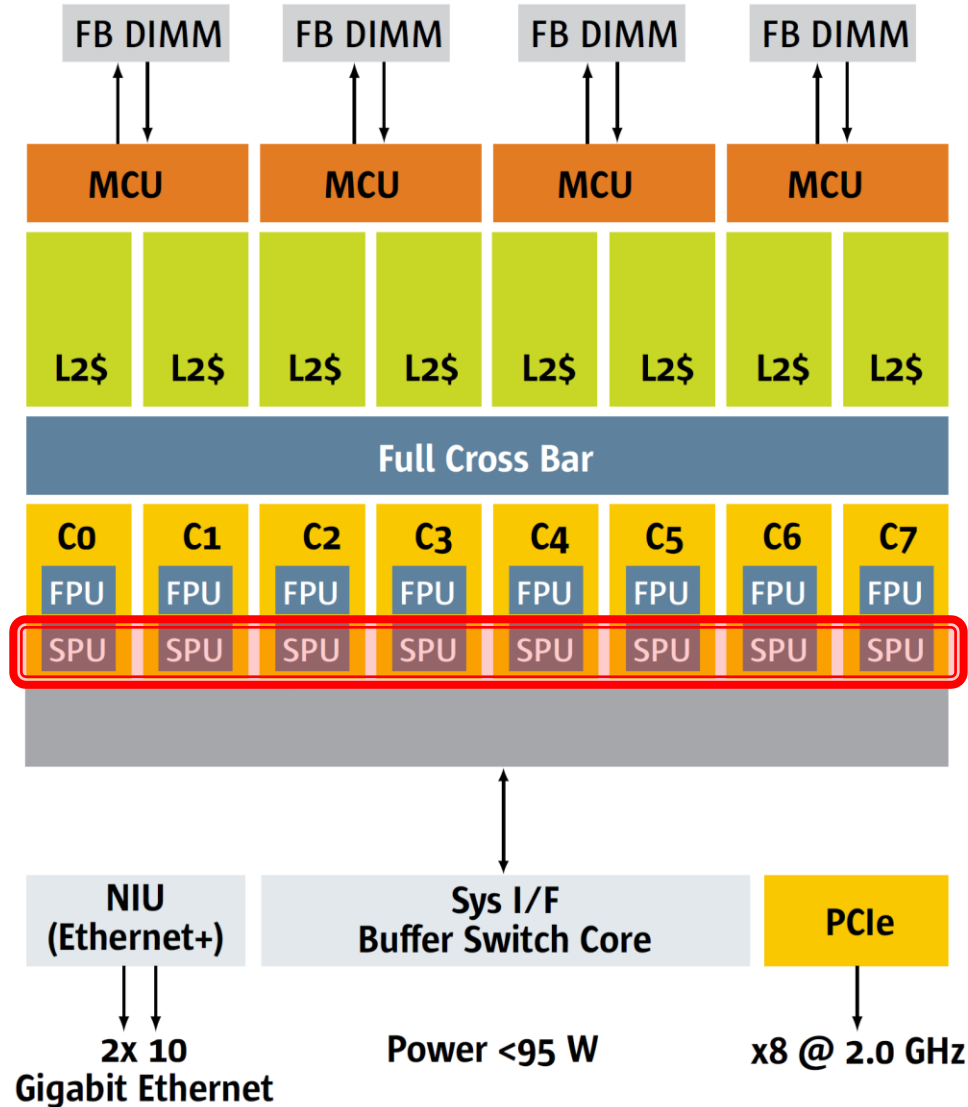
Rodina SPARC – kdo z nás ji vůbec zná?
(Super/Hyper/UltraSPARC *.* , SPARC64 *.*)

Všechny procesory Sun Microsystems šifrují!

Jsou to:

- Sun UltraSPARC T1 „Niagara“
- Sun UltraSPARC T2 „Niagara 2“
- Sun UltraSPARC T2+ „Victoria Falls“

[ooo] Sun UltraSPARCT2



[001] Urychlovače výpočtů

- [000] Procesory
- [001] Urychlovače výpočetního výkonu
- [010] Mainframe
- [011] Šifrovací doplňky
- [100] Pevné disky
- [101] Streamery a jejich média
- [110] Likvidace datových médií
- [111] Bezpečnost bez šifrování

[001] Urychlovače výpočtů

Kdo z nás si nepřál je mít v počítači?

Nešifrují... zato ďábelsky rychle!

IBM Cell, IBM PowerXCell 8i

Toshiba SpursEngine

ClearSpeed

NVIDIA akcelerátory

~~ATI~~/AMD akcelerátory

[001] IBM Cell, PowerXCell 8i

IBM Cell

IBM PowerXCell 8i

Sony PlayStation 3

IBM BladeCenter QS20, QS21, QS22

IBM Roadrunner

FixStars GigaAccel 180 (PCI Express x16)

výkon až 180 GFLOPS (jednoduchá přesnost)

[001] FixStars GigaAccel 180



[001] Toshiba SpursEngine

SpursEngine SE1000 je „ořezaný“ IBM Cell:

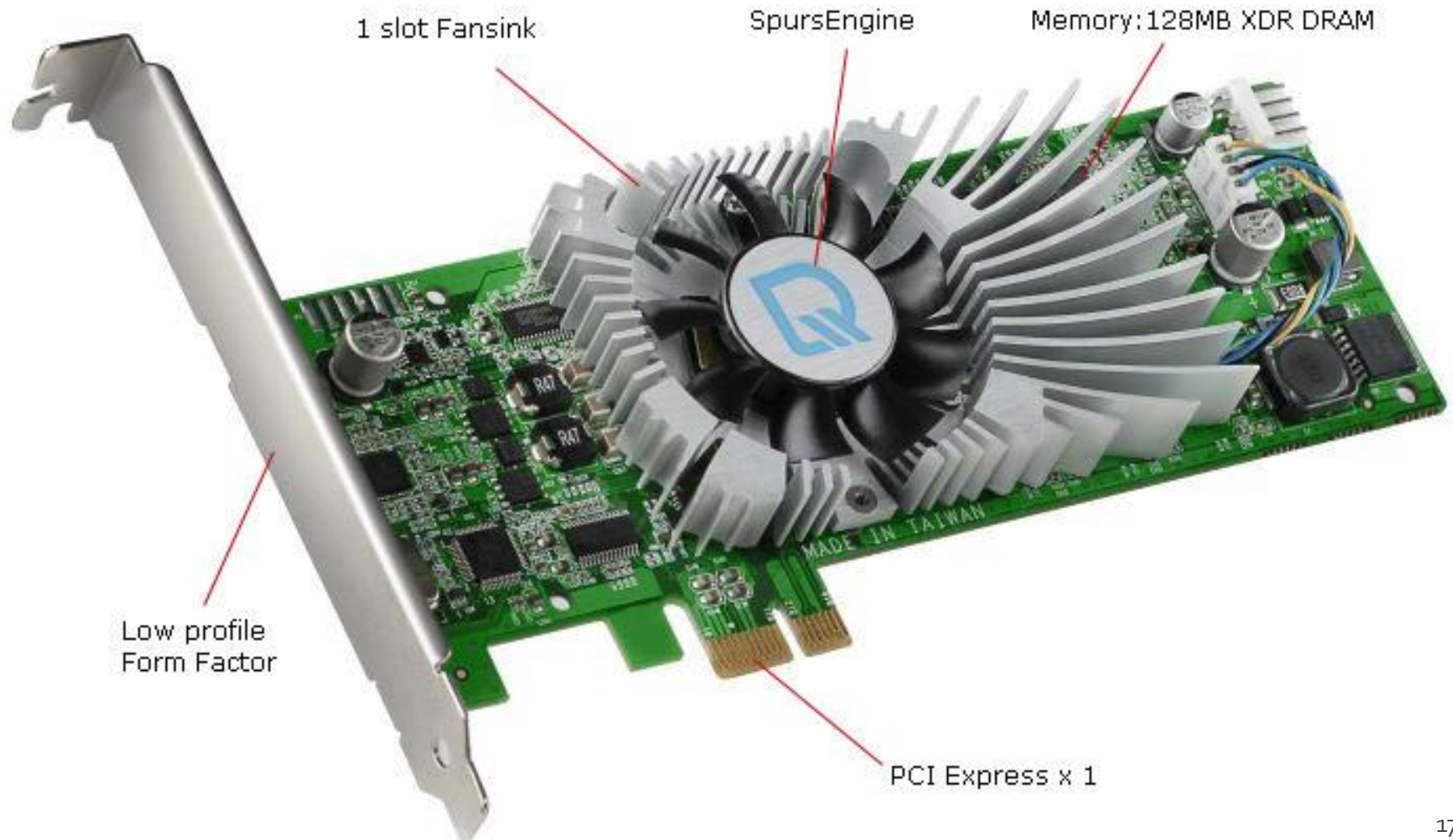
- chybí 4x SPE, chybí PowerPC
- zůstaly 4x SPE
- přibyl kodek videa

Toshiba Qosmio G50-10T (a další notebooky)

Leadtek WinFast PxVC1100 (PCI Express x1)

Thomson-Canopus Firecoder Blu (PCIe x1)

[001] WinFast PxVC1100

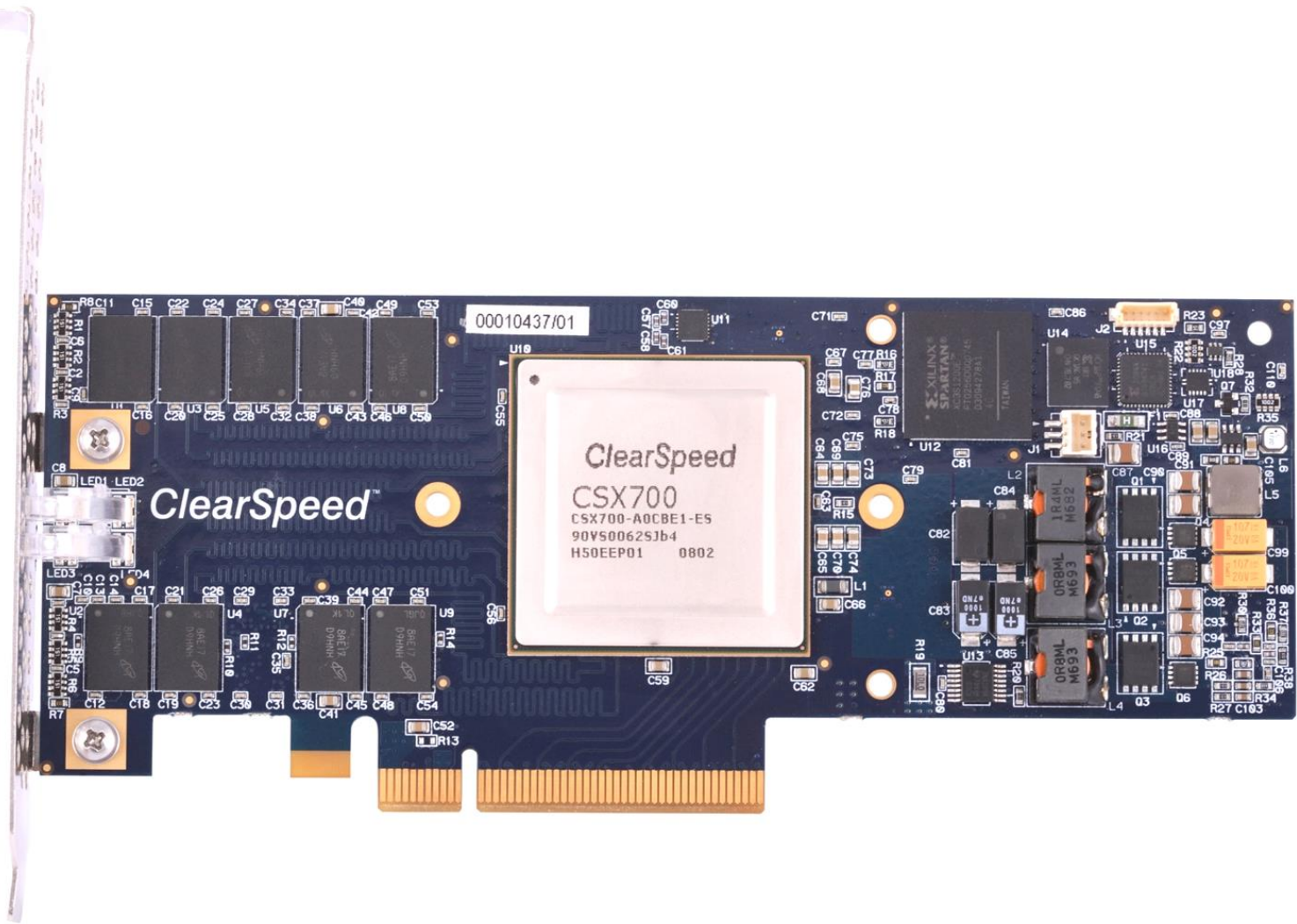


[001] ClearSpeed

Specializované karty s brutálním výpočetním výkonem

karty PCI-X nebo PCI Express x8
modul pro blade server Hewlett Packard

[001] ClearSpeed Advance e710



[001] GPU NVIDIA/AMD/S3...

GPU má obrovský výpočetní výkon.

Jak na něj?

Nejdále se dostala NVIDIA CUDA.

Vytvořil se „NVIDIACentrismus“

Je zapotřebí společné prostředí

[001] Urychlovače výpočtů

Kdo z nás si nepřál je mít v počítači?

IBM Cell, IBM PowerXCell 8i

Toshiba SpursEngine

ClearSpeed

NVIDIA akcelerátory + NVIDIA CUDA (?)

AMD akcelerátory (~~Stream~~)

cokoli z předchozího + **OpenCL** (!)

[010] Mainframe

- [000] Procesory
- [001] Urychlovače výpočetního výkonu
- [010] Mainframe
- [011] Šifrovací doplňky
- [100] Pevné disky
- [101] Streamery a jejich média
- [110] Likvidace datových médií
- [111] Bezpečnost bez šifrování

[010] Mainframe

Stále existují!

Spolehlivost, výkon, bezpečnost

Hardwarové šifrování?

již v IBM System/370 (od června 1970)

kompatibilita dodnes!

(IBM eServer zSeries, IBM System z)

[010] Procesor IBM z6

IBM z6 (viz IBM System z9) šifruje hardwarově!

Algoritmy:

DES (DEA, TDEA₂, TDEA₃)

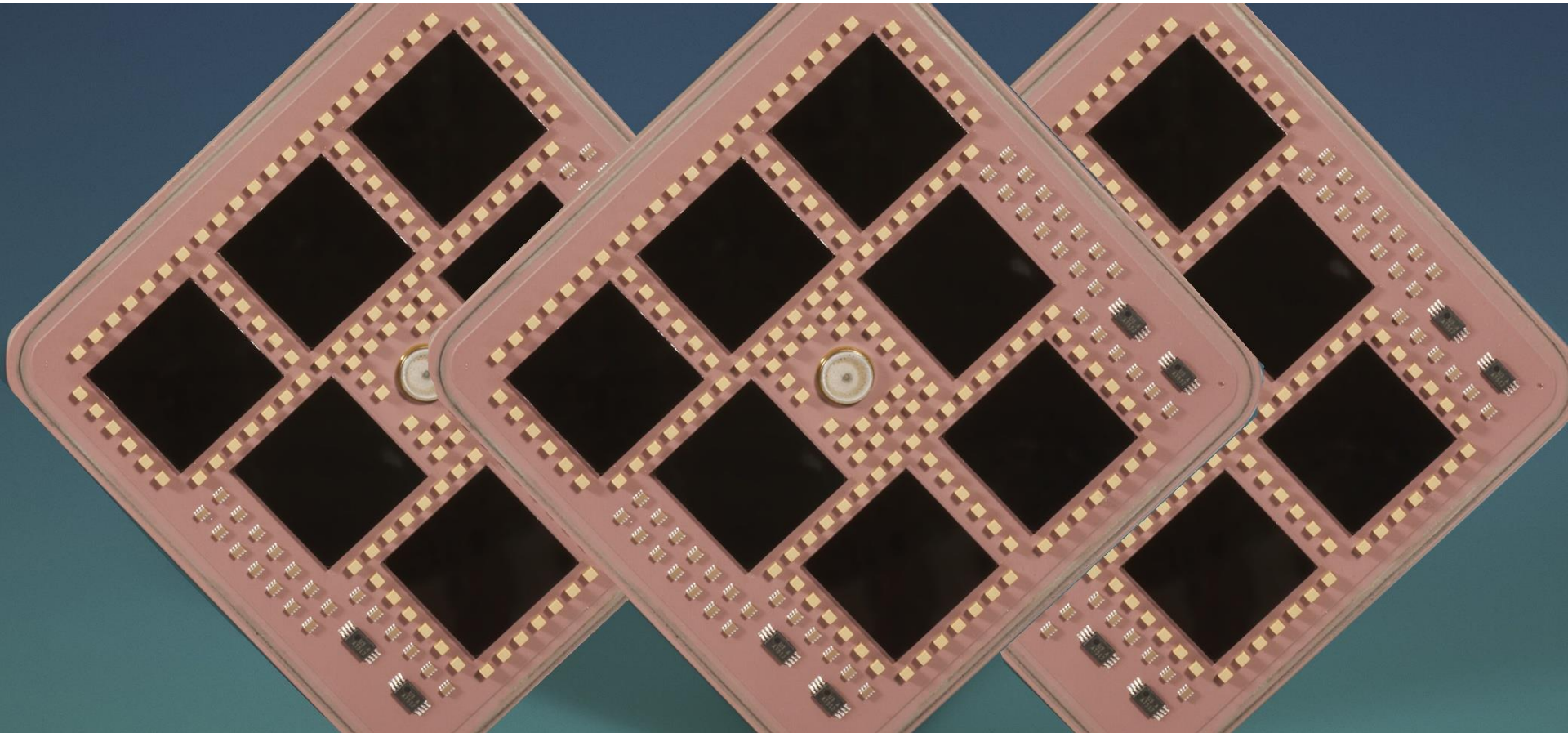
SHA-1 (160 bitů)

SHA-2 (256, 384 či 512 bitů)

AES (128, 192 nebo 256 bitů)

Šifrování rychlostí 290 až 960 MB/s

[010] Procesor IBM z6



[010] IBM System z10



[011] Šifrovací doplňky

- [000] Procesory
- [001] Urychlovače výpočetního výkonu
- [010] Mainframe
- [011] Šifrovací doplňky
- [100] Pevné disky
- [101] Streamery a jejich média
- [110] Likvidace datových médií
- [111] Bezpečnost bez šifrování

[011] Šifrovací doplňky

Šifrování je možné zrychlit i samostatnými součástkami.

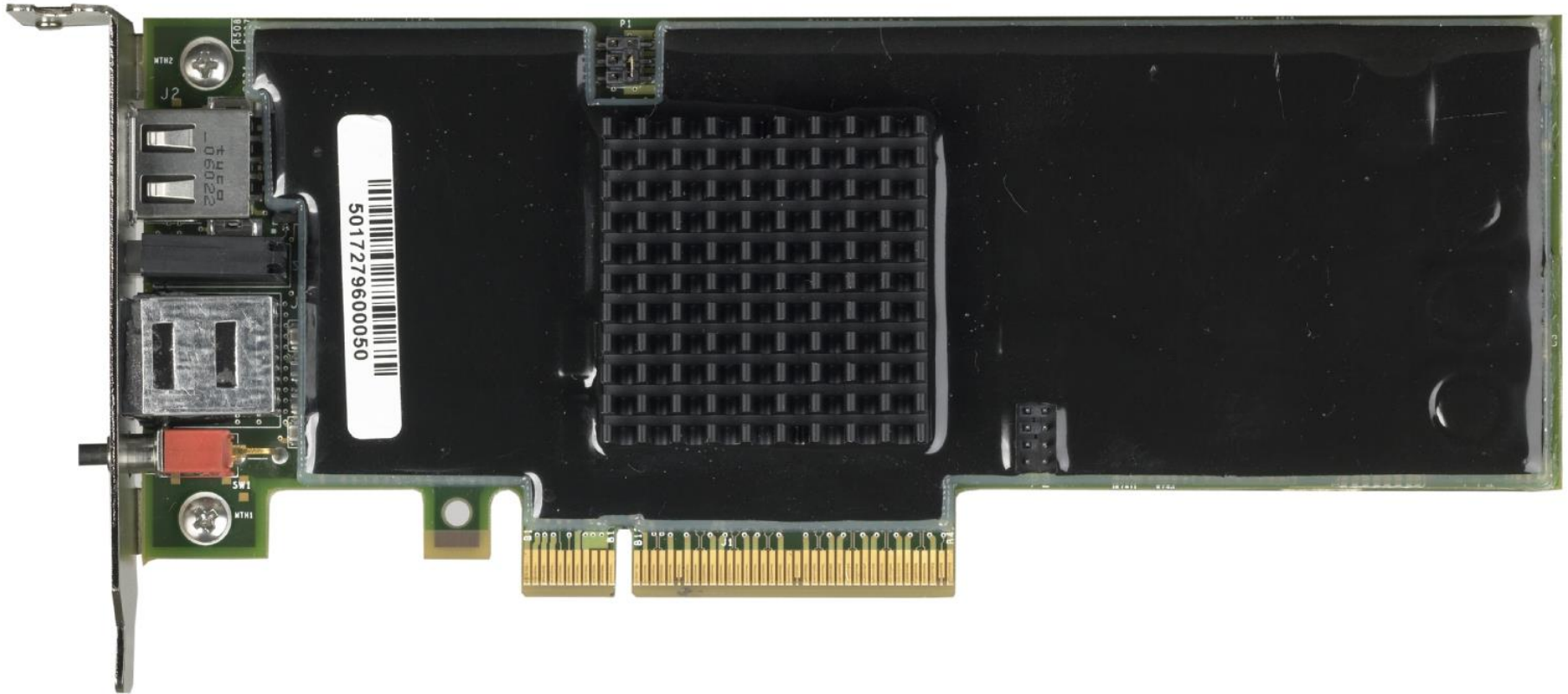
Discretix (DxAES a další)

IBM PCI/PCI-X Cryptographic Accelerator

Sun Crypro Accelerator 6000 PCI-E Adapter

- pro PCI Express x8
- až 13 000 RSA za vteřinu
- low profile (pro servery)

[011] Sun Crypto Acc. 6000 PCI-E



[100] Pevné disky

- [000] Procesory
- [001] Urychlovače výpočetního výkonu
- [010] Mainframe
- [011] Šifrovací doplňky
- [100] Pevné disky
- [101] Streamery a jejich média
- [110] Likvidace datových médií
- [111] Bezpečnost bez šifrování

[100] Pevné disky s šifrováním

Klasické rotační disky mohou šifrovat! Které?

Fujitsu:

- MHZ2xxxCJ (pro notebooky)
- MJA2xxxCH (pro notebooky)

Hitachi BDE

Seagate FDE/SED:

- Momentus (2,5" pro notebooky)
- Savvio (2,5" pro servery)
- Cheetah (3,5" pro servery)

[100] Seagate Savvio 15K



[101] Streamery a jejich média

- [000] Procesory
- [001] Urychlovače výpočetního výkonu
- [010] Mainframe
- [011] Šifrovací doplňky
- [100] Pevné disky
- [101] Streamery a jejich média
- [110] Likvidace datových médií
- [111] Bezpečnost bez šifrování

[101] Streamery a jejich média

Ukládání dat na pásky obnáší 2 problematiky:

- šifrování
- komprese

Tradiční proces:

- šifrování (počítač, hardwarově)
- komprese (streamerová mechanika)

Problém! Objem dat se nezmenší, protože jsou šifrovaná ☹

[101] Šifrující streamery

Mohou streamerové mechaniky šifrovat?

ANO!

Kompresa + šifrování proběhne v mechanice v reálném čase (např. až 350 MB/s).

IBM System Storage TS1120 model E05 a další
Sun Storagetek Crypto Ready T10000

[101] IBM System Stor. TS1130



[110] Likvidace datových médií

- [000] Procesory
- [001] Urychlovače výpočetního výkonu
- [010] Mainframe
- [011] Šifrovací doplňky
- [100] Pevné disky
- [101] Streamery a jejich média
- [110] Likvidace datových médií
- [111] Bezpečnost bez šifrování

[110] Likvidace dat a jejich médií

Stav média?

- provozuschopné
- nejsou provozuschopné

[110] Přepisování dat

Existují programy, přepisující data tolikrát, aby se šance obnovit data minimalizovala

Algoritmy jsou schváleny mnoha úřady:

- ministerstva (obraný apod.)
- armády
- rozvědky a jiné bezpečnostní útvary

[110] Výmaz dat

Magnetické nosiče je možné mazat magnetickým polem.

Pozor! Jedná se o likvidaci dat na úrovni obchodní bezpečnosti (nikoli vojenské atd.)

viz demagnetizátor Fujitsu MagSURE ME-P3

[110] Likvidace média

Obvykle nejúčinnější je zlikvidování samotného datového média (pevné disky, streamerové pásky, optická média apod.).

Speciální stroje:

- skartátory (samotná média)
- likvidace pevných disků (plotny jsou **ze skla**)

[110] BOW Industries MHDD

Before



After



[111] Bezpečnost bez šifrování

- [000] Procesory
- [001] Urychlovače výpočetního výkonu
- [010] Mainframe
- [011] Šifrovací doplňky
- [100] Pevné disky
- [101] Streamery a jejich média
- [110] Likvidace datových médií
- [111] Bezpečnost bez šifrování

[111] Bezpečnost bez šifrování

Obvykle se problémy vrší:

- firmware
- (virtualizace)
- operační systém + ovladače
- systémový software
- aplikace

Jak se problémy obvykle řeší? Další vrstvou

[111] Bezpečnost bez šifrování

Proč se neuvádí 100 %, nýbrž číslo blížíící se?

Proč nechtít opravdových 100 %?

[111] Bezpečnost bez šifrování

Spojení dvou počítačů dohromady bez datového propojení, případně pouze jednosměrně

Klíčová myšlenka?

Řešení je POD existujícím hardwarem. Proto není možné jej ovlivnit žádným softwarovým prostředkem.

[111] Bezpečnost bez šifrování

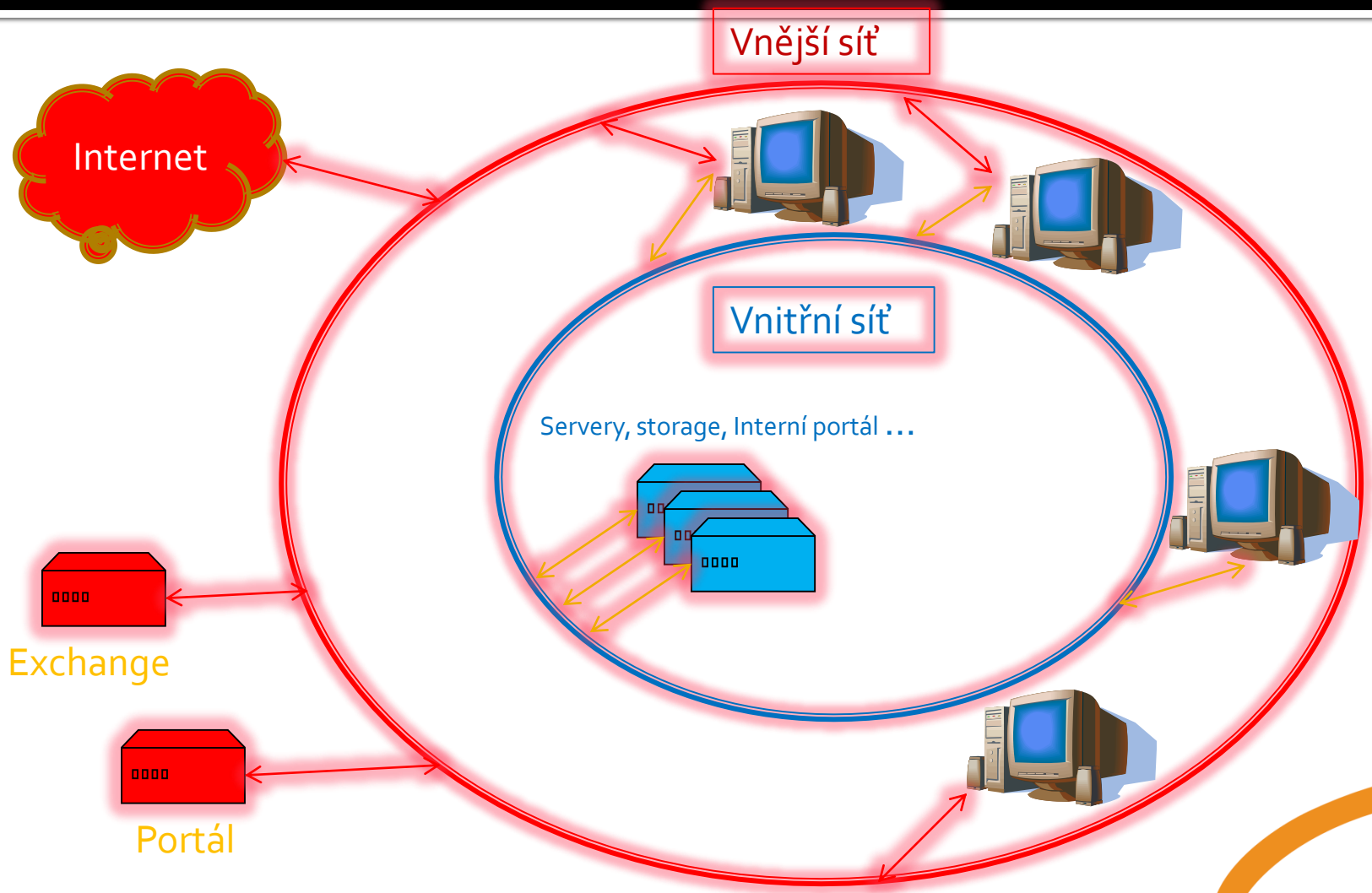
Přesně na to se soustředí společnost
PositronLabs.

Datová dioda (data tečou jen jedním směrem)

MLA (Multi Level Architecture)

MLW (Multi Level Workstation)

[111] Bezpečnost bez šifrování



ZÁVĚR

Bezpečnost je důležitá. Software se používá.

..ale jen **s hardwarem** ruku v ruce budeme **rychlí**

ZÁVĚR

Děkuji za pozornost!

Patrik Veselík

pveselik@muzeumpocitacu.cz