Třetina kryptografických čipů generuje slabé RSA klíče, prolomení je snadné

TPM čipy společnosti Infineon v posledních pěti letech obsahují vážnou bezpečnostní chybu, která vede ke slabým RSA klíčům. Tyto čipy jsou součástí notebooků, routerů, ale i šifrovacích tokenů.

PETR KRČMÁŘ | Dnes | **ŠIFROVÁNÍ** | **8 / 5**

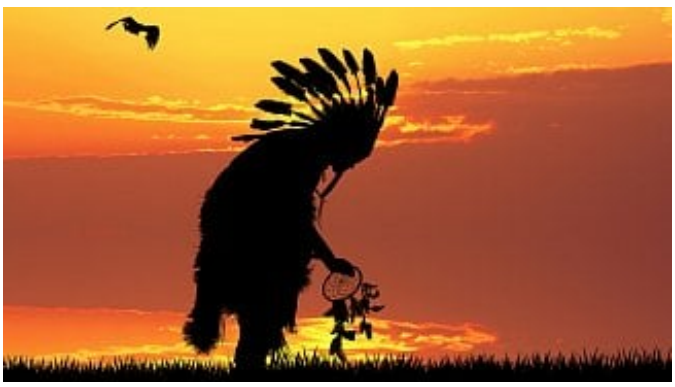
Tipy redakce

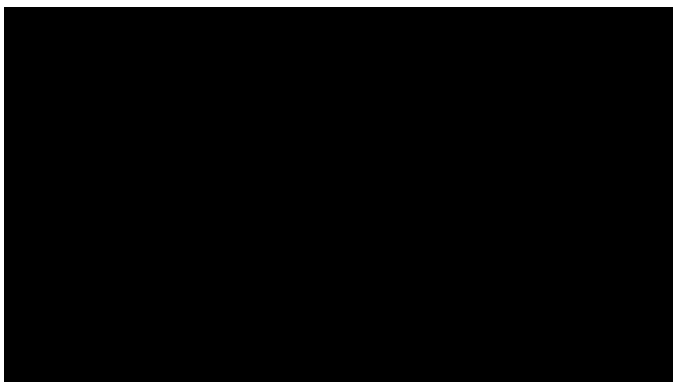
Foto galerie z LinuxDays 2017 (neděle)

Foto galerie z LinuxDays 2017 (sobota)

Rozšíření prohlížečů jsou hrozbou pro soukromí uživatelů

ČLÁNKY





Apache přidává podporu Let's Encrypt, pro HTTPS stačí jeden řádek konfigurace

Mozilla financovala vývoj modulu pro webový server Apache, který se tak brzy naučí přímo podporovat certifikáty od Let's Encrypt. Abyste své weby zpřístupnili po HTTPS, stačí přidat jednu konfigurační volbu.

PETR KRČMÁŘ

Dnes | **WEBOVÉ SERVERY** | 12

Softwarová sklizeň (18. 10. 2017)

Sonda do světa otevřeného softwaru. Dnes se podíváme na GUI pro síťového sniffera, vyzkoušíme nástroj pro převod formátů, začneme pracovat s terminálem trochu efektivněji a nakonec si připneme oblíbené stránky do docku.

JIŘÍ SLUKA

Dnes | **SKLIZEŇ**

Co přinese jubilejní ročník konference o mobilní komunikaci?

Na Mobile Internet Foru vás čekají přednášky o mobilní síti 5G, mobilním webu a aplikacích, NB-IoT sítích i eSIM.

Dnes

Tvorba grafického uživatelského rozhraní v Pythonu: dokončení popisu widgetů v knihovně appJar

Ve třetím článku o knihovně appJar dokončíme popis widgetů, které tato knihovna nabízí. Bude se jednat o užitečné doplňkové widgety – posuvník, zobrazení průběhu činnosti, widget pro výběr data apod.

PAVEL TIŠNOVSKÝ

Včera | **VÝVOJÁŘSKÝ SOFTWARE** | 2

Šifrování WPA2 prolomeno, Wi-Fi sítě je možné odposlouchávat (aktualizováno)

Aktualizováno včera 8:06

Několik bezpečnostních problémů bylo objeveno v šifrovacím protokolu WPA2, který je dnes velmi často používán na Wi-Fi sítích. Útok byl nazván KRACK a umožňuje odposlech i podvržení informací.

PETR KRČMÁŘ

16. 10. 2017 | **BEZPEČNOST** | **129**

Veřejný vs. privátní peering: argumenty na obou stranách

V komunitě peeringových koordinátorů se o tématu veřejného vs. privátního peeringu hodně diskutovalo. V této kapitole si představíme nejsilnější argumenty na obou stranách diskuze.

REDAKCE

16. 10. 2017 | **PŘIPOJENÍ K INTERNETU**

FÓRUM

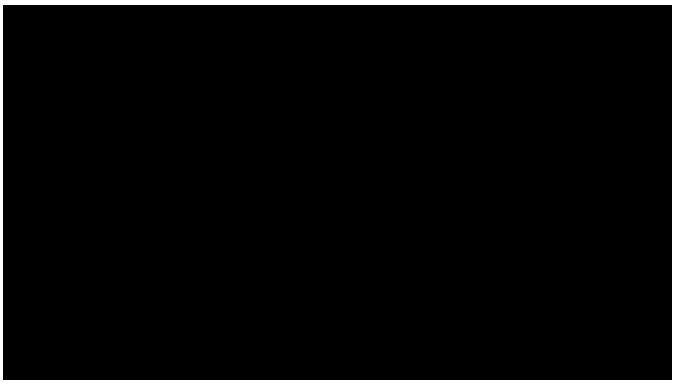
+ Nové téma

Nejnovější **Nejdiskutovanější** **Práce**

Jak eliminovat MITM pri overovani hesla postfixem (pri odesilani emailu)?	13:19
Prodám ODROID-XU4	13:11
CoolPeople - zkušenosti	13:02
Musí WPA2 zranitelnost opravit AP i klient?	12:43

Nový Root již dnes?	12:00
Jak synchronizovat dva freemailové účty	12:00
Tisk článků z root.cz v Chrome: chybí obrázky	12:00
Kde levně koupit 10GbE síťovky	12:00
Jak se vzdělávat jako vývojář?	11:56
Malý domací server	11:50
Má cenu si kupovat router Turris Omnia?	9:52
Bankovní systémy Unicredit Bank CZ	9:39
Jak správně zálohovat data okolo 20 GiB	7:30
CZ/SK, EU a patent	6:34
Význam ISO při focení do RAW	1:03
Živnost v Česku bez trvalého pobytu	Včera
Zdroje pro naučení ASP.NET	Včera
Nextcloud po upgradu: chyba integrity	Včera
Chodí vůbec na akce typu Javadays někdo koho nepošle firma? A proč?	Včera
Jakou klávesnici pro linux	Včera

Více témat

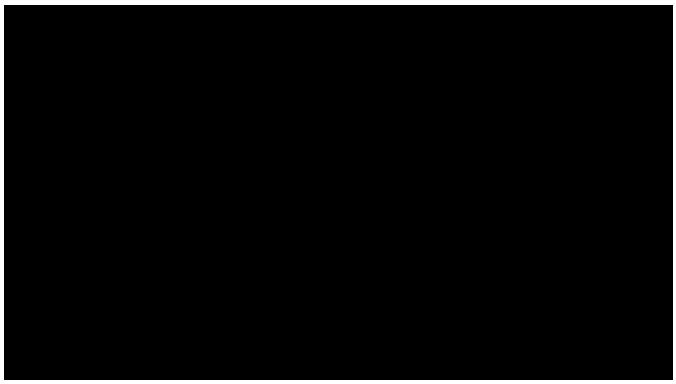


Postřehy z bezpečnosti: (ne)přizpůsobiví hackeři

V dnešním díle postřehů se podíváme na skupinu (ne)přizpůsobivých hackerů měnících techniky útoků, potenciální zranitelnosti 4G/5G sítí, Apple ID hesla v ohrožení a další zajímavosti z bezpečnosti.

CESNET CERTS

16. 10. 2017 | **BEZPEČNOST** | **5**

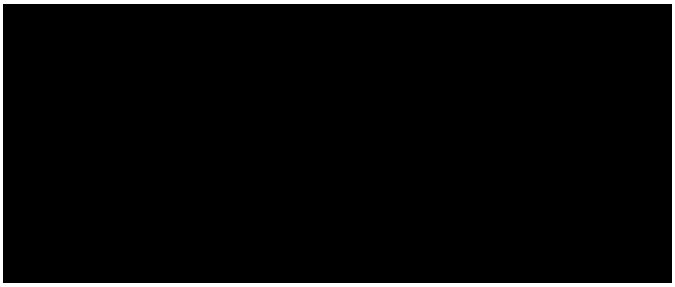


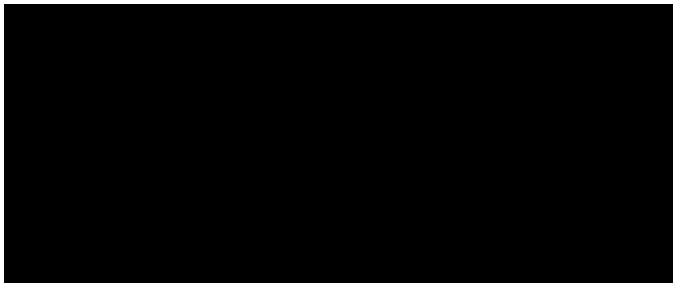
Intel má kvantový čip s 17 qubity, Western Digital slibuje 40TB disky

Western Digital slibuje 40TB disky díky technologii MAMR, Intel už má kvantový čip s 17 qubity, Microsoft se o kvantové počítání také zajímá a čím dál více webů nasazuje těžbu kryptoměn jako alternativu k reklamě.

DAVID JEŽEK

15. 10. 2017 | **STALO SE** | **46**





Komiks: preventívny

Niektoré dni sú tak náročné, že po príchode z práce koketujeme s myšlienkou na panáka. Mnohí sa dostanú aj ďalej. Určite čakáte nejaký edukatívny koniec. Ten však príde na druhý deň aj sám.

JANA SLEBODNÍKOVÁ

14. 10. 2017 | **HUMOR** | **32**

HEIF jako nástupce JPEG? Nemusí to stihnout

S novou generací iPhonů a novou verzí iOS se objevila i podpora formátu HEIF u mobilních produktů Applu, která přichází i do dalších aplikací. Má díky Applu HEIF šanci odstavit letitou vládu JPEGu na vedlejší kolej?

DAVID JEŽEK

13. 10. 2017 | **VIDEO** | **28**

Payment Request API: informace o platební kartě bezpečně v prohlížeči

Proč vyvíjí W3C standard, který bude přímo konkurovat PayPalu? Jakou má motivaci snažit se o to, aby placení na internetu bylo co nejrychlejší a nejpohodlnější? A co vlastně určuje akční rádius takové organizace?

MICHAL ČERNÝ

12. 10. 2017 | **BEZPEČNOST** | **72**

Machine Learning Weekend v Brně

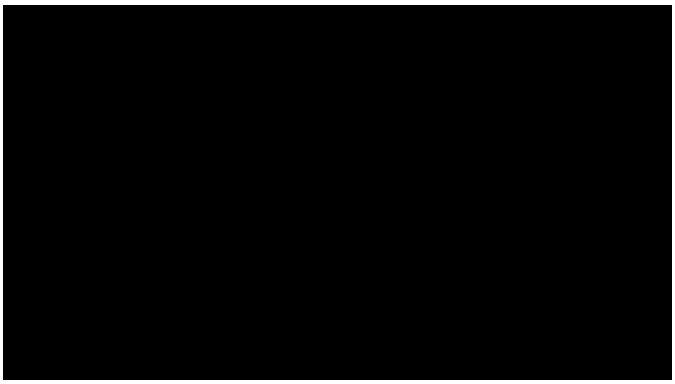
Intenzivní kurz strojového učení Machine Learning Weekend pod vedením top ML inženýrů se uskuteční 27.–29. října v Brně. Náplní kurzu budou základní kategorie strojového učení, jako je například zpracování přirozeného jazyka, umělé neuronové…

Torch: framework pro strojové učení i pro zpracování vektorů a tenzorů

Dnes se seznámíme s vlastnostmi frameworku Torch, který je používaný v oboru strojového učení, ale i pro „obyčejné“ zpracování vektorů a tenzorů. Pro psaní skriptů se používá Lua, interně je ovšem postavený na C.

PAVEL TIŠNOVSKÝ

12. 10. 2017 | **VĚDA A VÝZKUM** | **5**

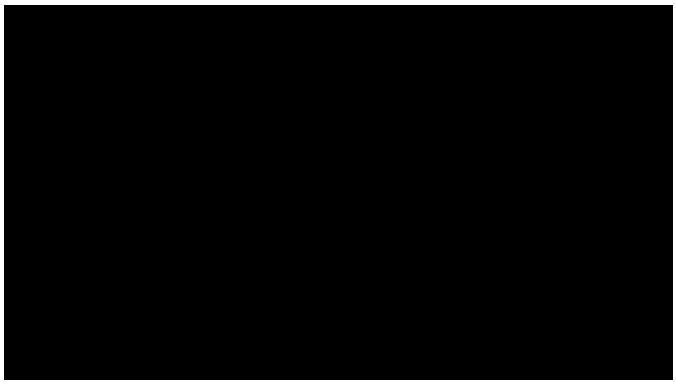


HiDPI v Linuxu: podpora se zlepšuje, kazí ji staré aplikace a frameworky

Už několik měsíců mám Dell XPS 13, který má tzv. HiDPI displej. Ten má vskutku impozantní jemnost: 3200×1800 pixelů na 13,3", což je hustota 276 pixelů na palec. Jak si s takovými displeji poradí linuxový desktop?

JIŘÍ EISCHMANN

11. 10. 2017 | **DESKTOP** | **62**



Softwarová sklizeň (11. 10. 2017)

Sonda do světa otevřeného softwaru. Dnes si zašifrujeme složky, vyzkoušíme klienta pro svobodnou sociální síť, přehrajeme si pár písniček a podíváme se na další systém na správu obsahu.

FILIP ZATLOUKAL

11. 10. 2017 | **SKLIZEŇ** | **3**

Root.cz (www.root.cz)
Informace nejen ze světa Linuxu. ISSN 1212-8309