



cena 99 Kč / 149 Sk
Únor - 02/2006

LinuxEXPRES

OPRAVDOVÝ LINUXOVÝ MAGAZÍN



Software pro PDA
čtečky / přehrávače / knihy

Michael Simms
Linux Game Publishing

Blender
Pro 3D modelování

6020office
Kancelář se zárukou

AVG 7.1
Antivir zdarma



Vývoj jaderných modulů
Programovací jazyk Eiffel
Pracujte v Bashi - seriál
Bittornado na torrenty

Deset ukázkových
stran tohoto čísla
najdete na
www.linuxexpres.cz.

Elektronické předplatné: LinuxEXPRES také jako PDF!



Red Hat

Mono ve Fedoře

Projekt Mono, který je open-source implementací platformy .NET firmy Microsoft, se dočkal zařazení do vývojové větve Fedory a stane se tak součástí jejího dalšího, v pořadí pátého, vydání. Bude zahrnut do jádra distribuce, což kromě jiného znamená snadnou instalaci a používání v příštím vydání Red Hat Enterprise Linuxu. Jeho zahrnutí přímo do enterprise distribuce je ale stále velmi nepravděpodobné. Překvapivá opatrnost ohledně tohoto kroku (Fedora je patrně jednou z posledních všeobecně užívaných distribucí, která projekt Mono zahrnuje) mohla být motivována kromě jiného i tím, že Mono je sponzorováno především konkurenční firmou Novell.

Red Hat nejprínosnější

Každoroční anketa mezi řediteli pro informační technologie významných amerických firem, organizovaná vydavatelstvem Ziff Davis (Ziff Davis' CIO Insight Research Study), vyhlásila již podruhé za sebou firmu Red Hat za nejprínosnějšího dodavatele v oblasti informačních technologií. Na dalších dvou místech se umístily firmy Apple a Cisco. Red Hat získal nejvyšší ocenění především v oblastech realizace plánovaných úspor, návratu vynaložených prostředků a výhledů na další možnou spolupráci. Studie měla k dispozici odpovědi od 884 manažerů a mezi hodnocenými oblastmi byl dále přínos ve formě růstu výnosů a schopnost vyřešit daný problém.

Nový ředitel pro IT

Novým ředitelem pro informační technologie firmy Red Hat se stal Brian Stevens. Stejný post zastával ve firmě Mission Critical Linux, což byla firma založená bývalými zaměstanci firmy Compaq, resp. Digital. Oproti většině ostatních nově příchozích manažerů z poslední doby je Brian Stevens dobře znám především pro své schopnosti softwarového architekta a inženýra, které osvědčil během své dlouholeté kariéry, ať už jako jedna z hlavních postav vývoje Tru64 Unixu (operační systém pro řady VAX a Alpha firmy Digital). Mezi další jeho počiny patří i práce na vývoji první komerční implementace X Window Systemu, který byl vyvíjen jako součást projektu Athena, což byl pokus o vznik distribuovaného desktopového výpočetního prostředí, na němž se podílely firmy Digital, IBM a akademici z MIT a který byl spuštěn v roce 1983(!). Za svou existenci tomuto projektu vděčí kromě jiného i dnešní X Window, instant messaging a Kerberos technologie.

Stanislav Poláček

Zdroj: www.linworx.cz

Výkonný editor v Javě

Program jEdit si již stihl získat hodně příznivců, ale mnoho lidí ho stále ještě nezná – a je to škoda, protože jeho schopnosti jsou vskutku vynikající. Na první pohled se neliší od mnoha jiných podobných editorů, ale pod kapotou se skrývá mohutný agregát. jEdit má prakticky vše, co můžeme od editoru očekávat – snadné a efektivní ovládání, rozsáhlé editační schopnosti (včetně různých formátovacích funkcí a regulačních výrazů), zvýraznění syntaxe obrovského množství jazyků, bohatou konfigurovatelnost a mnoho dalšího.

To nejdůležitější se ale skrývá jinde – v makrech a zásuvných modulech. Již po instalaci je v programu k dispozici několik maker pro časté operace a lze si vytvořit svá makra podle potřeby. Pomocí zásuvných modulů si lze přidat téměř jakoukoli schopnost. Mnoho modulů již existuje (např. CSS editor, generátor HTML z kódu, FTP klient, nástroje pro LaTeX, práce s obrázky), další si lze vytvořit.

Milovníci programů vim a Emacs svým oblíbeným asi sbohem nedají, ale kdo rád edituje v grafickém prostředí, měl by určitě jEdit vyzkoušet. Jeho kvality za to stojí, a to i přesto, že je to program napsaný v Javě, která u některých lidí není příliš oblíbená.



Divoce ohnivá komunikace

Když se řekne Wildfire Server, asi to málokomu něco řekne. Není divu, tento program se původně jmenoval jinak – ale hlavně, spadá do kategorie trochu méně známé. Je to totiž server pro komunikační technologii XMPP, známé spíše pod názvem Jabber.

XMPP serverů existuje celá řada, nicméně tento má dvě charakteristické vlastnosti: je napsán v Javě a kompletně se konfiguruje a ovládá přes webové rozhraní. Pro toho, kdo chce velice rychle rozjet server pro tento druh komunikace, je to dobrá volba. Není potřeba nic složité zkoumat ani editovat konfigurační soubory, prostě se program nainstaluje (lze stáhnout včetně JVM

i samostatně), nastartuje se server a už to jede. Vše potřebné se nastaví přes prohlížeč. Protože mezi podporovanými jazyky je i čeština, snadnější už to snad být nemůže.



Nějaké vady na kráse program má – jednak jsem mezi dostupnými doplňky nenašel brány pro přístup do jiných IM sítí, dále se po změně konfigurace musí obnovit stránka, aby se zobrazovalo aktuální nastavení, a konečně má server na můj vkus až příliš vysoké nároky na výkon počítače. Proto pro nasazení do prostředí s mnoha uživateli asi nebude příliš vhodný, ale pro menší skupiny komunikujících uživatelů se Wildfire jeví jako výborné řešení.

Lukáš Jelínek

<http://www.jedit.org>
Domovská stránka editoru jEdit

<http://www.jivesoftware.org/wildfire/>
Server WildFire

Sudoku pro palm

Asi jste si již všimli v novinách nebo jinde nového fenoménu – číselných křížovek, kterým se říká *sudoku*. Pokud jste příznivci sudoku a zároveň vlastníkem nějakého palmu, možná vás bude zajímat program Sudoku od Andrewa Gregoryho, který vám nyní představím. Ačkoliv je tento projekt jen něco přes půl roku starý, umí toho i při necelých 90 kB docela dost – skoro vše, co mobilní řešitel sudoku k radosti potřebuje.



Michael Simms, riaditeľ spoločnosti Linux Game Publishing

Na súčasnosť a budúcnosť linuxového herného priemyslu sa pýtal Michal Spáda.



Mohol by si na úvod povedať našim čitateľom niečo o sebe a o svojich spoločnostiach?

Tux Games som založil v roku 2000, keďže milujem Linux a keďže milujem hry. Chcel som začať robiť niečo, pri čom by som sa mohol realizovať v oboch týchto oblastiach. Neskôr, v roku 2002, som založil *Linux Game Publishing*, lebo som vedel že s *Lokim* to ide dolu vodou a bolo mi jasné, že ak niekto iný nezačne vydávať hry pre Linux, *Tux Games* nebudú mať čo predávať!

LGP sa za posledné roky snaží hlavne rásť a pritom produkovať kvalitné hry. V súčasnosti sme už vydali deväť titulov, takže sa pomaly dostávame tam, kde by sme chceli byť. V tomto roku by sme radi vydali niekoľko nových titulov pre Linux, z ktorých niektoré sme už oficiálne ohlásili a niektoré sú momentálne ešte tajné - aspoň zatiaľ.

Čo sa týka mňa osobne, nenapadá mi nič, čo by som o sebe zúfalo túžil ľuďom povedať, ale ak máš nejaké otázky, sem s nimi.

O autorovi:

Michal Spáda (*1980) študuje doktorský program na katedre anglistiky FF UP v Olomouci. V práci (tiež na univerzite) i doma používa výhradne Linux a FreeBSD. Hranie a vývoju hier sa venuje vo voľnom čase.

Pravdu povediac, myslím, že naši čitatelia budú spokojní, ak im prezradíš, ktorú distribúciu používaš, či máš radšej GNOME, alebo KDE, vi alebo Emacs, a tak podobne.

Ok, čo sa týka distribúcie, používam Fedoru - som užívateľom Red Hatu od verzie Red Hat 3 a zatiaľ som nepocítil potrebu prejsť niekam inam. Ako desktop používam GNOME 2 kombinovaný s Enlightenment. Som jeden z tých, ktorí sa spoliehajú výhradne na Emacs, na druhej strane som presvedčený, že by mal každý poznať vi aspoň do tej miery, aby si bol s jeho pomocou schopný Emacs nainštalovať.

V minulosti sme boli svedkami toho, ako hneď niekoľko herných spoločností, predovšetkým Loki Software, malo síce sľubný začiatok, ale neskôr sa z trhu úplne stratili. Boli ste v LGP väčší realisti pri predajných odhadoch?

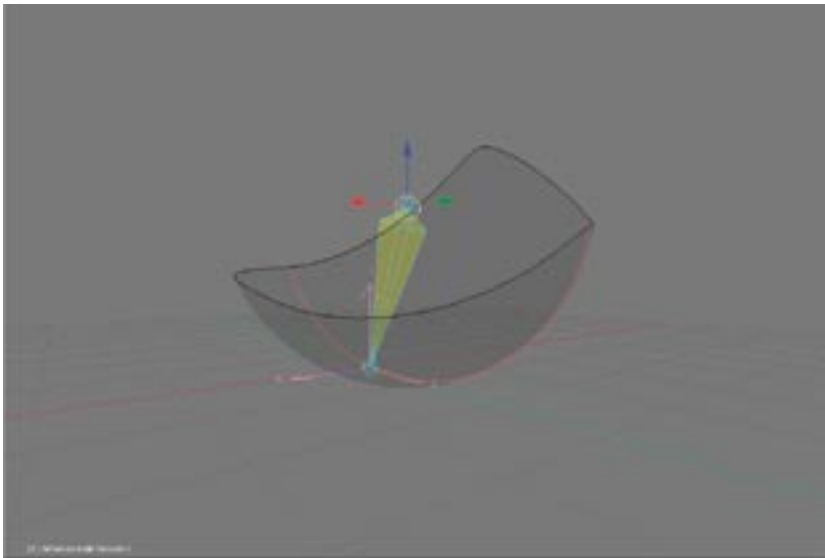
Nuž, dosť sme sa poučili z Lokiho chýb. Jedna z vecí, ktoré robíme inak, je to, že sa nesnažíme získať a portovať tituly s „veľkými“ menami, ku ktorým ale patria aj šesťciferné licenčné poplatky. Vyhľadávame hry, ktoré sa vyznačujú vysokou kvalitou, ale zároveň nepatria k tým úplne najznámejším. Týmto spôsobom sme schopní udržať náklady na úrovni, ktorá je proporcionálna k rozmerom trhu a zároveň umožňuje rast spoločnosti priamo úmerne s rastom počtu linuxových hráčov. Tituly, ktoré si napokon zvolíme, prechádzajú veľmi starostlivým výberom, kedy sa snažíme uistiť, že hoci sa nejedná o najznámejšie mená, sú to všetko vynikajúce hry, ktoré majú šancu osloviť naše publikum.

Práve na proces výberu budúcich portov by som sa ťa rád spýtal bližšie. Doteraz sa vám v tomto smere darilo, vydávate hry, ktoré nepatrili na pôvodnej platforme medzi trháky, ale väčšinou mali veľmi pozitívne ohlasy, predovšetkým čo sa týka hrateľnosti. Ktoré faktory teda pri výbere portu zohľadňujete?

Program si môžete stiahnuť z oficiálnej stránky blender.org, kde nájdete spolu so zdrojovými kódmi aj modifikácie pre viaceré operačné systémy a architektúry procesorov. To ocenia najmä majitelia strojov s architektúrou PowerPC, či už na ňom prevádzkujú Linux, alebo MacOS X.

Technika, využívaná pri animácii pomocou kostry, pri ktorej podradené kosti ovplyvňujú nadradené, sa dočkala taktiež mnohých zlepšení. Áno, hovorím o inverznej kinematike (*Inverse Kinematics*). Spôsob jej aplikovania bol značne zjednodušený a samozrejme pribudli aj nové možnosti. Ako takmer všetky časti programu, aj táto sa môže pýšiť zrýchlením výpočtov, a to zásluhou novej stromovej štruktúry všetkých kostí, vďaka ktorej sú výpočty podradených kostí patriacich spoločnej nadradenej prevádzanej spolu a celkovo sú rýchlejšie.

Jednou z nových možností je vymedzenie rozsahu otáčania kostí okolo jednotlivých osí, ktoré nájde využitie, napríklad pri zabránení ohnutiu kolena postavy dopredu alebo jeho iným neprirodzeným pohybom. Ak je toto rozpätie definované v dvoch dimenziách, v tom prípade je zobrazované v podobe časti elipsoidu.



Vizuálne zobrazenie rozsahu možného otáčania kosti.

Shape keys, alebo u konkurencie nazývané *Morph targets*, sú neodmysliteľným nástrojom nielen na poli vizualizácie mimických pohybov. Pracujú na základe interpolácie pozícií jednotlivých vertexov (morfovanie) vrámci jedného objektu. Informácie o ich pozíciách nazývané kľúče (*Absolute vertex keys*), môžete ľubovoľne zlučovať a taktiež vytvárať prechody medzi požadovanými z nich.

Pomocou štetca je teraz možné morfovanie medzi vybraťmi skupinami vertexov, ktoré sa nachádzajú v poli jeho pôsobenia. Podobne ako mnoho ostatných funkcií sa aj táto dočkala lepšej integrácie do grafického rozhrania a odteraz ju štandardne nájdeme na rovnakom paneli ako modifikátory; panel sa nachádza medzi editovacími funkciami.

Pribudla nová interpolačná metóda Bézierových kriviek v IPO editore, ktorá ošetruje presah animačnej krivky za kontrolnú úsečku. Interpretácia takýchto kriviek v trojrozmernom priestore je totiž v drvivej väčšine prípadov odlišná ako v IPO editore. V súčasnosti je nová metóda

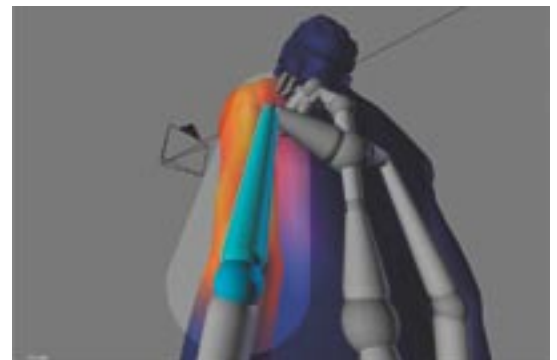
použitá pri vkladaní kľúčovej snímky štandardne, no jej predchodkyňa, rovnako ako aj ďalšie metódy, je dostupná tiež a môžeme ju aplikovať cez menu, alebo rýchlejšie, pomocou klávesovej skratky.

Problémom nástrojov prevádzajúcich logické operácie so sieťami modelov (Boolean tools) vždy bolo, že v niektorých prípadoch bola vzniknutá sieť modelu veľmi nerovnomerná, čo bolo spôsobené pridávaním nadbytočných vertexov. Riešenie prináša taktiež jeden z projektov, ktorý spomenutý nedostatok odstraňuje, a tak výsledný model má čo najmenšie množstvo polygónov. Je to významná úprava, pretože Boolean tools patria medzi veľmi často používané nástroje.

Jednou z najzaujímavejších záležitostí je nepochybne Fluid Simulation, teda funkcie na simuláciu pohybu kvapaliny. Za ich pomoci je možné vizualizovať správanie sa rôznych druhov kvapalín od bežnej vody až po med. V prospech tohto nástroja svedčí verné napodobenie správania sa kvapalín na základe ich fyzikálnych vlastností, no na druhej strane musíte počítať s enormne vysokými nárokmi na operačnú pamäť počítača.

Za spomenutie určite stojí aj novinka zvaná *verse*, ktorej implementáciu prevádza Jiří Hnídek. Tento protokol na výmenu dát fungujúci na báze klient-server umožňuje vymieňať dáta v reálnom čase medzi najrozšírejšími 2D a 3D grafickými nástrojmi. Pre ostatné programy (Maya, 3ds Max, atď.) bude *verse* dostupné v podobe pluginu.

Revolučným by som nazval spôsob vytvárania vlasov a chlupov, ktorý pochádza z dielne animačného štúdia Orange. Spočíva v použití natiahnutých polygónov usporiadaných kolmo vzhľadom na pohľad kamery. Ich realistickosť je na veľmi vysokej úrovni, no nevyriešeným problémom aj naďalej zostáva ich rendering, ktorý je nadmerne náročný na systémové prostriedky. Dúfajme, že sa jeho zrýchlenia dočkáme v najbližšom čase.



Renderovanie síce trvá dlho, ale výsledok rozhodne stojí za to.

Niektoré funkcie boli združené a teraz sú dostupné vo výstúvacom zozname v podobe modifikátorov z jedného panelu. Táto na prvý pohľad kozmetická úprava výrazne uľahčuje ovládanie prostredia programu. Všetky modifikátory majú totiž zjednotený vzhľad aj spôsob použitia. Je možné ich

Pre Linux je dostupná dynamická a statická verzia. Rozdiel medzi nimi je v tom, že tá prvá menovaná využíva knižnicu rozhrania OpenGL, ktoré musíte mať nainštalované v systéme, pričom statická ich má už prilinkované, takže odpadá niekedy zdĺhavý proces ich inštalovania. Na druhej strane, statická nedokáže využiť OpenGL akceleráciu na hardvérovej úrovni.

tvorit ikonu na ploše nebo odkaz v hlavní nabídce. Je možné doinstalovat i dodaný kalendář nebo jiná (např. z internetu stažená) rozšíření.

U 602SQL stačí nainstalovat jeden RPM balíček. Pro jeho integraci s OOo je ale potřeba ještě rozbalit SDBC ze zip archivu a nainstalovat jej. Toho lze dosáhnout jak pomocí grafického prostředí OOo, tak s použitím textového nástroje k tomuto balíku dodávanému. Další podrobnosti jsou popsány v dokumentaci.

Běhové prostředí Java je nutné pro fungování některých částí balíku OOo (např. modul Base). Nejprve zkopírujeme soubor `bin` na pevný disk. Potom mu nastavíme práva spouštění (např. pomocí `chmod 755 jre...bin`) a soubor spustíme (`./jre...bin`). Zobrazí se licenční podmínky a pokud s nimi vyslovíme souhlas, rozbalí se RPM balíček.

Na CD je ještě zmíněný převodník souborů z 602PC Suite do OOo, který však funguje pouze pod MS Windows. Pokud by nějaký uživatel Linuxu přece jen potřeboval jeho služeb využít, doporučuji vyzkoušet spuštění této aplikace s pomocí Wine.

602SQL95

Nebudu se zabývat popisem aplikací OOo a Thunderbirdu, protože ty jsou většinou uživateli dobře známy a jsou volně k dispozici. Soustředím se hlavně na proprietární prvek balíku 602Office, kterým je databáze 602SQL95 a věci s ní související.

Jde skutečně o plnohodnotnou multiplatformní SQL databázi s podporou XML. Dokáže mimo jiné spolupracovat s OOo, ODBC, JDBC a PHP. Po instalaci se objeví v hlavní nabídce v sekci *Kancelář* jako *Server 602SQL95*. Lze jej spustit také příkazem `602sql95 -n602office_db`, kde `602office_db` je jméno databáze.

Řeknete si, že není třeba utrácet za něco, co lze nahradit svobodnými MySQL, PostgreSQL či Ingres? V tom případě byste měli vyzkoušet *Klient 602SQL95*, který pod tímto jménem najdete v nabídce *Kancelář*, nebo jej můžete spustit příkazem `602gcli95`.

Tato aplikace je vytvořena pomocí GTK a umožňuje pomocí pohodlného grafického rozhraní ovládat databázový server, vytvářet, spravovat a prohlížet databáze, ale také tvořit databázové aplikace. Jde tedy o komplexní klientské vývojové prostředí plně lokalizované v češtině.

Jeho ovládání je do značné míry intuitivní. Např. pro vytvoření uživatele, databáze, tabulky a její naplnění pár řádky dat jsem nepotřeboval žádnou nápovědu, natož dokumentaci. Přesto je škoda, že v dodané tištěné i elektronické dokumentaci je tento nástroj zmíněn jen okrajově.

Elektronická dokumentace

Dokumenty k 602Office si můžete stáhnout z internetu. Je jich pět (na webu jsou ještě doplňkové materiály) a jsou opravdu dobrými pomocníky. *Průvodce instalací kancelářského balíku 602Office 2* (27 stran) má samostatnou sekci věnovanou Linuxu, kde jsou příklady konkrétních příkazů pro instalaci na distribuci SuSE, které lze většinou použít i na ostatních distribucích využívajících RPM.

Základy práce s 602Office 2.0 (251 stran) není zrovna nejvýstižnější název, protože tato příručka se věnuje i pokročilejším tématům, jako je sledování změn v dokumentu, vnořené funkce v tabulkách apod. *Praktické příklady využití databáze v kancelářském balíku 602Office* (17 stran) a *Šablony smluv* (9 stran) se soustředí na konkrétní ukázky práce s databází, resp. šablonami, v OOo.

Pro uživatele migrující z balíku MS Office je jistě zajímavá poslední příručka – *Přechod z Microsoft Office na OpenOffice.org* (86 stran). Tento tzv. rozdílový manuál se věnuje převodu souborů, obecným rozdílům v uživatelském rozhraní i konkrétním odlišnostem jednotlivých aplikací. Kniha neobsahuje mnoho snímků obrazovky, zato však nabízí přehledné srovnávací tabulky funkcí a klávesových zkratk.

PDF jsou zpracována kvalitně. Není problém zobrazit je v xpdf, kpdf či Evince. Položky obsahu fungují jako odkazy na příslušné části textu. Jen snímky obrazovky mohly být pořízeny ve větším rozlišení a nemusely všechny pocházet jen z prostředí MS Windows.

Zhodnocení

Projekt 602Office je zhmotněním myšlenky komerční podpory pro otevřený a svobodný kancelářský balík, v daném případě OOo. To je určitě dobrá zpráva pro všechny příznivce svobodného softwaru a otevřených datových formátů, protože je to nutnou podmínkou širšího nasazení těchto technologií v praxi.

Tato iniciativa zřejmě není zaměřena na nenáročného uživatele nebo naopak dobré znalce OOo a svobodných implementací SQL. Zakoupení 602Office však mohou vřele doporučit každému, kdo chce nasadit OOo ve firmě. Užitečný je také pro náročnější uživatele, kteří ocení dodávané šablony, galerii tisíců obrázků anebo profesionální databázi 602SQL. ■

Odkazy:

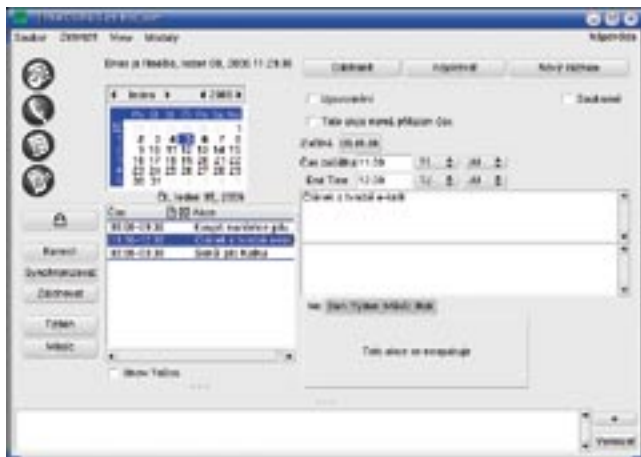
<http://www.software602.cz>
Software 602

http://www.602.cz/cz/produkty/602office_2_0/dokumentace
Stážení dokumentace

Poslední součástí produktu 602Office jsou doplňkové služby. Klíčem k nim je distribuční číslo přiložené v krabici i se základními instrukcemi. Registrací na webu získáte roční uživatelskou podporu, tj. řešení problémů prostřednictvím e-mailu s přístupem ke znalostní databázi, nové verze produktu, přístup k dokumentaci, šablonám, diskusnímu fóru, informacím a novinkám.

Galerie obsahuje 6463 obrázků JPEG o velikosti většinou do 300x300 bodů. Jsou rozříděny do více než deseti kategorií, které se však částečně překrývají. Sbírkou je doplněna o katalogy sdv a thm, takže ji lze podstrčit OOo nakopírováním do adresáře
~/.openoffice.org2/user/gallery/.

Sbírkou šablon sestává především z 58 souborů `ott` rozdělených do adresářů na smlouvy k nemovitostem (nájem, podnájem, věcné břemeno, ...), smlouvy občansko-právní (kupní, příkazní, půjčka, ...), obchodní (mandátní, o dílo, vedení účtů, ...), pracovní (DPP, DPČ, hmotná odpovědnost, ...).



Internetem nedávno probleskla zpráva, ve které bylo řečeno, že součástí KDE verze 4 bude nová aplikace se starým názvem **KitchenSync**. Tato aplikace vyjde z již existujícího programu OpenSync a bude sloužit jako jakási univerzální rozhraní pro PDA s různými operačními systémy. Už v roce 2006 by měla umět komunikovat s Palm OS a poté ji její autoři budou učit společnou řeč s dalšími platformami. Vývoj KPilotu nebude zastaven. Program ale přestane být součástí KDE.

O autorovi:

Lubomír Čevela (*1968) je programátorem na volné noze. Kromě používání Linuxu patří mezi jeho zájmy především fotografování a práce s videem.

Odkazy:

<http://www.jpilot.org>
Domovská stránka aplikace J-Pilot

http://www.slac.com/pilone/kpilot_home/
Domovská stránka aplikace KPilot

<http://gnukeyring.sourceforge.net>
Domovská stránka aplikace Keyring

poznámky 4 kB přesně podle staršího provedení Poznámek v přístrojích Palm OS kompatibilních. Novější modely Palmů umožňují délku poznámky až 32 kB. Pořídíte-li si tedy na nich poznámku přesahující 4 kB, v J-Pilotu ji získáte oříznutou. To je dle mého mínění vaši nervovou soustavu ohrožující nedostatek. Malou náplastí je fakt, že pokud do poznámky nezasáhnete v J-Pilotu, bude zkrácena jenom v něm a nikoli ve vašem palmu.

J-Pilot podporuje zásuvné moduly Expense (výdaje), Keyring (chráněná databanka hesel), SyncTime (synchronizace času palmu a desktopu) a MailSync (synchronizace zpráv elektronické pošty). Z nich je nejzajímavější Keyring, který v konkurenčním Palm Desktopu ani v KPilotu nemá svůj protějšek. Keyring je aplikace pro uložení důvěrných údajů. Jeho databáze je šifrována silnou šifrou 3x DES a chráněná vstupním heslem. K dalším nezbytným vlastnostem J-Pilotu patří zálohování obsahu paměti palmu a samozřejmě jeho obnovení z pořízené zálohy.

Mírná nevýhoda J-Pilotu oproti KPilotu a taktéž oproti originálnímu Palm Desktopu resp. HotSyncu je v postupu synchronizace u palmů vybavených USB portem. Nejprve je nutné spustit synchronizaci na straně palmu a až zhruba dvě vteřiny poté můžete stisknout tlačítko „Synchronizovat“ v J-Pilotu. Pořadí je nutné dodržet kvůli aktivaci USB ovladačů jádra resp. usbilib.

Hlavní výhoda J-Pilotu je v možnostech jeho nastavení. To kromě jiného obsahuje obousměrnou konverzi mezi znakovými sadami ISO-8859-2 a Palm Windows1250 (EE). Nastavíte-li si tuto konverzi a máte-li lokalizaci svého palmu nastavenou na kódovou stránku Windows 1250, můžete střídavě synchronizovat palm s okenním Palm Desktopem a s linuxovým J-Pilotem, přičemž česká diakritika bude v obou případech zachována.

KPilot

Už z názvu KPilotu je možné rozpoznat jeho příslušnost k aplikacím oblíbeného desktopového prostředí KDE. Nikoho tedy asi nepřekvapí použití grafické knihovny Qt a licencování licencí GNU

GPL. KPilot má oproti J-Pilotu velkou výhodu při synchronizaci s palmem.

Pro start synchronizace není nutné používat žádné jiné tlačítko než to na vašem palmu nebo na jeho kolébce. Leč každá výhoda je vyváжена nějakou nevýhodou, a tak obousměrnou konverzi znakových sad v KPilotu nehledejte. Buďto bude používat váš palm kódovou stránku ISO-8859-2, nebo se budete muset obejít bez české diakritiky. Střídavá synchronizace s okenním Palm Desktopem je tedy možná, ale bez zachování češtiny. Na rozdíl od víceméně monolitického J-Pilotu vytvořili KPilot jeho autoři spíše jako soubor rozhraní mezi palmy a standardními součástmi KDE. Kalendář a úkoly zajišťuje aplikace KOrganizer, poznámky si bere na starost aplikace KNotes. Kontakty mohou být synchronizovány s Knihou adres a nebo také s groupwarovým klientem Kroupware. Sestavu rozhraní KPilotu doplňují zásuvné moduly Propojení s Avant GO, Synchronizace dokumentů ve formátu Palm DOC, Synchronizace času a Install Files – instalace souborů do palmu.

KPilot stejně jako J-Pilot umožňuje zálohovat obsah vašeho palmu a v případě hard resetu jej obnovit. Problém zkracování poznámek delších než 4 kB se bohužel projevuje i u něj. Velice vítaným doplňkem je možnost synchronizace dokumentů ve formátu Palm DOC. Škoda, že ji znehodnocuje nemožnost volby české kódové stránky. Na rozdíl od skálopevně stabilního J-Pilotu je KPilot padavější. Ačkoli jsem ho používal poměrně krátkou dobu, okno s nabídkou odeslání bugreportu jsem viděl víckrát, než mi bylo milé.

Celkové porovnání

J-Pilot a KPilot dokáží originální Palm Desktop bez větších problémů nahradit. Pokud vaše PDA vybavené Palm OS nepotřebujete synchronizovat střídavě s linuxovým desktopem, s okenním Palm Desktopem a jste-li sžiti s PIM aplikacemi z prostředí KDE nebo používáte-li Kroupware, pak je pro vás KPilot tou nejlepší volbou. V opačném případě zvítězí J-Pilot na celé čáře.

V porovnání se současným Palm Desktopem chybí oběma jeho linuxovým protějškům multimediální rozšíření o synchronizaci fotografií, rukou kreslených poznámek (NotePad) a hlasových poznámek. A to nepočítám synchronizaci s kancelářským balíkem Documents to Go. Faktem je, že tato rozšíření je možné snadno nahradit přímým přístupem na paměťovou kartu z vašeho PDA pomocí čtečky karet. Celkově je tedy spolupráce palmů s linuxovými desktopy mírně omezenější než s originálním Palm Desktopem, větší na uživatele ale nebude nic podstatného postrádat. ■

takže umí jen několik málo rozlišení s konkrétními frekvencemi, takže ten rozřádkovaný obraz byl nejspíš 800x600.

To, že mám takový speciální monitor, nemůže ABC Linux samozřejmě vědět, Sun žádné DDC signály neumí. Ale LCD je umí, a tak si konfigurátor mohl z monitoru přečíst, že nativní rozlišení je 1280x1024. Poslední výtkou je, že nebyla zapnutá Xinerama. Na obou monitorech bylo zvlášť spuštěné KDE. Zvláštní je, že na sekundárním monitoru (Matrox) byly zapnuté „efekty myši nad ikonou“ v hlavním panelu KDE, na primárním se zobrazují jen obyčejné žluté obdélníčky.

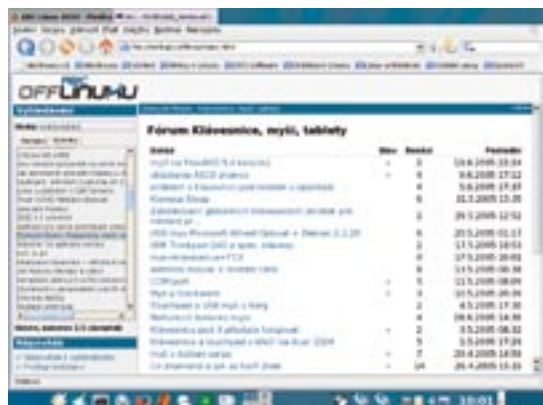
Moje konfigurace zjevně ABC Linux zaskočila, ale na druhou stranu, valná většina uživatelů má jen jeden monitor a ať chceme, nebo ne, 1024x768 je tak nějak použitelné všude. Snad jen ta Xinerama mohla být zapnutá. Přepsal jsem si tedy ručně rozlišení na 1280x1024, odstranil jsem konfiguraci druhé karty a jel jsem dál.

Na notebooku s displejem 1024x768, který se ale hlásí jako 800x600 (vada notebooku) se mi grafické prostředí spustilo v 800x600. Možná by opravdu bylo lepší na autodetekci zapomenout a před spuštěním se zeptat na několik základních věcí, jako je např. rozlišení.

Spuštění KDE

V ABC Linuxu 2005 je na výběr KDE a Fluxbox. KDE je všeobecně známé těžkotónažní prostředí a naopak Fluxbox je tak minimalistický, jak to jen jde. Fluxbox je určen spíše pro pokročilé uživatele, zaměřím se tedy především na prostředí KDE.

V systému je uživatel `guest` s heslem `guest` a pod tímto uživatelem se i KDE spustí. Oproti Slaxu se grafický režim spouští ihned, samozřejmě pokud si uživatel při startu nezvolí režim textový. V systému je samozřejmě i `root` a i pod ním lze grafické prostředí spustit, nicméně to nelze doporučit. Rozdíly jsou minimální, snad jen, že `guest` má pozadí v modré barvě



a `root` ve žluté, grafický motiv a i vše ostatní je stejné.

Prostředí KDE

Na dolní liště je zleva řada ikon s často používanými programy, přepínač ploch, volné místo, ikonka s disketou, tray a hodiny. Kupodivu chybí přepínač otevřených oken, ten se totiž schovává pod horním okrajem plochy. Jelikož jsou CD distribuce zaměřené především na stávající uživatele Windows, tuto drobnost hodnotím záporně, je to trochu nezvyklé. Samozřejmě není problém si do volného místa ten přepínač oken přidat a ten nahoře zrušit.

Na ploše pak jsou víceméně standardní ikony z KDE, tedy *Můj adresář*, *Systém* a *Média*. Dále pak ikona *Vítejte*, kde jsou užitečné informace o ABC Linuxu a nesmí chybět ikona *AbcLinuxu.cz offline*, která spouští Firefox s offline mirrorom mateřského webu. A nakonec tři adresáře: IBM, Novell a Stickfish, kde se nacházejí reklamní materiály od sponzorů. Jejich jména jsou ostatně i napsána přímo na ploše.

Prostředí Fluxbox

Pokud budete chtít spustit ABC Linux 2005 na starém počítači nebo prostě nemáte rádi KDE, zkuste grafické prostředí Fluxbox. Je sice opravdu spartánské, ale v ABC Linuxu je nakonfigurováno prakticky stejně jako KDE, takže v menu, které se vyvolává pravým tlačítkem myši, jsou stejné programy jako v KDE, jen tam nejsou jejich ikonky. Spodní panel Fluxboxu je vlastně jen přepínač ploch, přepínač programů, tray a hodiny. Jednoduché, prosté a funkční.

Používáme ABC Linux 2005

Nemá smysl zde vypisovat jednotlivé programy nebo jejich verze, stačí, že CD je plné užitečných programů, mezi kterými nechybí Firefox, OpenOffice.org, manažer souborů Krusader, multimediální přehrávač Kaffeine a Beep Media Player, nesmí chybět ani ICQ klient Kopete nebo vypalovací program K3b.

S ABC Linuxem se mi pracovalo opravdu pěkně, systém byl opravdu velmi rychlý, až mě to překvapilo,



Rozhovor s Tomášem Matějčkem jsme přinesli také na stránkách LinuxEXPRESu, aktuálně jej najdete na adrese <http://www.linuxexpres.cz/rozhovor-tomas-matejcek>.

quash+unionfs – kombinace komprimovaného systému souborů s možností zápisu na média jen pro čtení, např. CD. Změny se zapisují pouze do paměti.

Kromě startu do prostředí KDE a Fluxbox lze také provést test paměti. Je to proces trvající v závislosti na množství RAM až několik hodin.

AGP je sběrnice grafických karet; někdy se může stát, že není správně inicializována. APM a ACPI jsou systémy pro správu napájení, jejich funkčnost často záleží na kvalitě BIOSu a také možnostech jádra (kernelu) linuxového systému.

DDC (Display Data Channel) je standard definovaný asociací VESA (Video Electronics Standards Association). Slouží k automatickému nastavení videorežimů adaptéru (monitoru).

Balíčkový program **pacman** je srdcem distribuce – tedy alespoň co se softwaru týče. Je také ostře sledovanou komponentou, uživatelé zhýčkaní **aptem** z Debianu nebo **emerge** z Gentoo jsou tvrdými kritiky.

Verze 0.7.1. Noodle byla 5. ledna 2006 vydána jako stabilní a byla založena nová vývojová větev 0.8, zatím bez jména.

Můžete si stáhnout i obraz 0.7 Wombat, po aktualizaci se systém sám přejmenuje na 0.7.1. Máte na výběr dva obrazy – *base* (obsahuje pouze základní systém) a kompletní CD s většinou dostupných balíčků.

Pokud máte rychlé připojení k internetu (alespoň ADSL), můžete použít pouze 0.7 base a stáhnout si z internetu další balíky v aktuální verzi. Verze 0.7.1 existuje na internetu také jako kompletní CD. Toto CD pak použijte v případě, že rychlé připojení nemáte k dispozici anebo neplánujete kompletní aktualizaci. Dále pak samozřejmě i v případě, že připojení k internetu nemáte k dispozici vůbec. Vzhledem k změnám doporučuji (je-li to možné) instalovat 0.7.1 (anebo novější 0.8).

rozdělení použijte pouze v případě, že máte prázdný disk, na kterém má být pouze Arch Linux. Tato volba totiž odstraní všechny existující oddíly a zabere celý disk pro Arch Linux. V případě ručního rozdělení pak můžete použít *fdisk* nebo o něco uživatelsky přívětivější *cfdisk*.

2. Výběr balíčků

Pokud instalujete z FTP, dostanete na výběr FTP zdroje. Je možné, že některé nebudou fungovat, takže se nebojte při neúspěchu stažení seznamu balíčků zkusit jiný. Nyní se vás program ptá, zda chcete pouze základní (*base*), nebo kompletní instalaci. Pokud máte k dispozici síť, je asi lepší nainstalovat nejprve *base* instalaci a teprve po restartu a nastavení systému doinstalovat vše další ze sítě. Rovněž máte-li k dispozici pomalejší připojení, pak nainstalujte základní systém z CD a vše další už si stáhněte ze sítě. Dále je zde možné, kromě skupin balíčků, požádat o detailní výběr jednotlivých balíčků. Po odsouhlasení skupin se vám tak objeví seznam jednotlivých balíčků. To doporučuji i pokud instalujete pouze základní systém. Můžete například odstranit balíky pro modemové a bezdrátové připojení, pokud jej nepoužíváte.

3. Instalace balíčků

Nyní následuje instalace balíčků, která může při instalaci z FTP trvat i delší dobu v závislosti na rychlosti vašeho připojení. Na průběh stahování se lze podívat na konzoli pět. Do ní se přepnete známou klávesovou zkratkou [Alt+F5], zpátky pak [Alt+F1]. Po dokončení stahování se na první konzoli zobrazí průběh vlastní instalace a případně informace o změnách konfiguračních souborů.

4. Výběr jádra

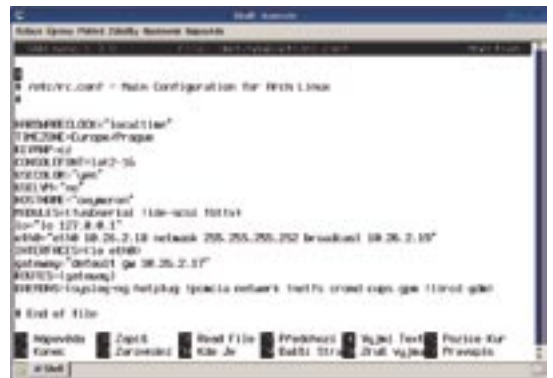
Následuje výběr jádra. Musíte si zvolit, jaké jádro chcete. Zda chcete jádro 2.4, nebo 2.6 – pokud nemáte nějaký specifický důvod (starý hardware), pak zvolte 2.6. V případě jádra 2.4 pak, zda chcete SCSI, nebo IDE. Dále si můžete i zvolit zdrojový kód jádra, přeložit si jej, což však doporučuji až v okamžiku, kdy budete mít fungující systém. Instalace jádra probíhá podobně jako instalace balíčků, na konzoli pět se můžete dívat na průběh stahování. Je použito co nejnovější jádro.

5. Konfigurace systému

Editace konfiguračních souborů. Nejprve máme na výběr, zda použijeme editor *vi*, nebo *nano*. Pokud ani jeden neznáte, zvolte *nano*, jehož ovládání je celkem intuitivní. Můžeme editovat následující soubory: */etc/rc.conf* – základní nastavení – lokalizace (fonty pro konzoli, klávesnice), síť, spouštění modulů

při startu, spouštění služeb při startu. Služby i moduly lze snadno vypnout přidáním vykřičníku před její jméno v seznamu. Např. pokud nepoužíváte DHCP, je třeba povolit bránu (gateway) a změnit v seznamu síťových služeb **!gw** na **gw**. Například budete-li chtít přidat do služeb *ssh*, pak stačí připsat kamkoliv mezi řádek se seznamem spouštěných služeb (**DAEMONS**) *ssh*. Pokud jej naopak nebudete chtít spouštět, není nutné slovo *ssh* mazat, stačí před něj napsat vykřičník.

/boot/grub.conf (anebo */etc/lilo.conf* – dle zavaděče, který chcete použít). */etc/fstab*, */etc/modprobe.conf* pro jádro 2.6, nebo */etc/modules.conf* pro jádro 2.4. */etc/resolv.conf* – zde



zapište cestu k DNS serveru (pokud jej potřebujete), případně jméno implicitních domén.

6. Instalace zavaděče

Musíte si zvolit, zda GRUB, anebo LILO. Nevíte-li co, doporučuji GRUB. Nezapomeňte editovat jeho konfigurační soubor - viz předchozí bod. Dále musíte zvolit, zda se bude instalovat do MBR, pokud to má být hlavní zavaděč systému, anebo na bootovací oddíl, pokud již nějaký zavaděč používáte. V druhém případě nezapomeňte upravit odkaz na tento disk v nadřazeném zavaděči.

7. Exit

Ukončení instalace. Pokud si uvědomíte, že jste na něco zapomněli, spusťte znovu */arch/setup*.

Po instalaci

Nyní již zbývá napsat **reboot**. Pokud je to nutné, upravte po restartu ještě externí zavaděč systému, jinak si počkejte na start zavaděče a vyberte Arch Linux (není-li defaultní). Během startu systému sledujte případné chyby, abyste je mohli po nastartování opravit. Trochu mne mrzí, že po zavedení systému startovací hlášky se zaváděním služeb zmizí, takže pokud dojde k chybě v poslední službě, skoro nemáte šanci si jí všimnout.

Vývoj jádra II.

– jednoduchý modul

Stačí pár řádků kódu, spustit kompilaci a modul zbývá jen načíst. Radí Lukáš Jelínek.

V minulém – prvním – dílu seriálu o vývoji součástí linuxového jádra jsme si shrnuli hlavní zásady, kterými by se měl každý vývojář řídit. Nyní přejdeme k samotnému vývoji. Na konci této kapitoly už by měl být každý schopen vytvořit, zkompileovat a načíst svůj vlastní modul.

Co je potřeba ke kompilaci modulů

V první řadě potřebujeme samozřejmě kompilátor. Není třeba žádný speciální – náš důvěrně známý *GCC* plně vyhovuje. Předpokládám, že už ho každý má ve svém systému nainstalovaný (což je ostatně nutná podmínka pro kompilaci běžných programů); pokud tomu tak není, stačí doinstalovat z distribuce a nejlépe také aktualizovat na poslední stabilní verzi (ať už 3.x.x, nebo 4.x.x).

Další podmínkou je přítomnost zdrojových souborů jádra. Ty lze získat z oficiálního serveru (*ftp.kernel.org*), bývají také v distribucích. Některé distribuce obsahují kromě plných zdrojů také „odlehčenou“ verzi – ta plně postačuje ke kompilaci modulů pro jádro, ke kterému přísluší, ale celé jádro z nich zkompileovat nelze. Pro experimenty stačí i tato odlehčená verze, v pozdějších fázích vývoje je lépe se uchýlit k plným zdrojovým textům.

Programový kód musíme mít samozřejmě v čem napsat. Lze použít libovolný editor (vim, Emacs, Kate, jEdit apod.) nebo vývojové prostředí (Eclipse + CDT, KDevelop, Anjuta, Sun Studio atd.) – je to čistě záležitost vaší volby a chuti.

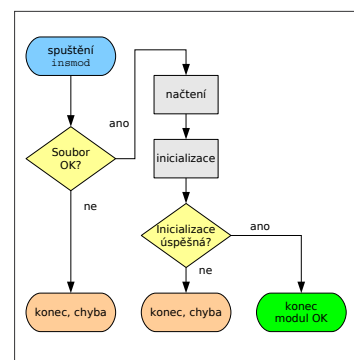
První kroky

Pro kompilaci nejjednoduššího modulu budeme potřebovat dva soubory. Samotný zdroják (prostě normální céčkovský soubor) a soubor *Makefile*. Postupně se na ně podíváme. Než k tomu ale dojde, bude dobré si připomenout, jak se s moduly jádra pracuje.

Uvažujme modul jako samostatný objekt, který máme někde na disku (typické místo pro nainstalované moduly je pod adresářem */lib/modules*), odkud ho můžeme načíst do paměti. Moduly lze načítat prakticky kdykoliv, lze je i uvolňovat (odstraňovat) za běhu jádra. Zda a jak to probíhá, záleží na konfiguraci jádra. Obvykle můžeme moduly načítat v libovolnou chvíli a uvolňovat je také kdykoliv (kromě doby, kdy je někdo používá).

Pro manipulaci s moduly máme dvě skupiny programů: nízkourovňové (*insmod*, *rmmod*) a „inteligentní“ (*modprobe*). Ty doplňují ještě programy s informativní funkcí (*lsmod*, *modinfo*). Nízkourovňové programy pouze tupě vykonávají svou činnost

– *insmod* zavede modul do paměti, *rmmod* ho uvolní. Program *modprobe* toho umí mnohem víc (a je také konfigurovatelný), v pravý čas se na něj podíváme podrobněji.



Stručné schéma práce programu *insmod*.

O autorovi:

Lukáš Jelínek (*1977) vystudoval FEL ČVUT v oboru Výpočetní technika. Žije v Kutné Hoře a pracuje jako vývojář softwaru pro různé platformy, včetně programů pro embedded systémy. Ve volném čase rád fotografuje, natáčí a stříhá video a také se věnuje (v Čechách poměrně málo známému) powerkitingu.

URL článku:

www.linuxexpres.cz/06s2

```

#include <linux/module.h>
#include <linux/init.h>

static int __init mymodule_init(void)
{
    printk(KERN_INFO "mymodule: modul inicializovan\n");
    return 0;
}

static void __exit mymodule_cleanup(void)
{
    printk(KERN_INFO "mymodule: modul uvolnen\n");
}

module_init(mymodule_init);
module_exit(mymodule_cleanup);

MODULE_LICENSE("GPL");
MODULE_DESCRIPTION("První zkusebni modul");
MODULE_AUTHOR("Lukas Jelinek <luk@php.net>");
  
```

Darwinia

Michal Spáda predstavuje najnovšiu hru od Introversion Software.

Technické požiadavky:

Jadro 2.4 alebo novšie,
glibc-2.1 alebo novšie,
X Window System
Procesor P3 600 MHz alebo lepší
128 MB RAM,
60 MB HDD
32 MB grafická karta
s 3D akceleráciou
OSS kompatibilná zvuková karta
(stačí emulácia cez ALSA)

O autorovi:

Michal Spáda (*1980) študuje doktorský program na katedre anglistiky FF UP v Olomouci. V práci (tiež na univerzite) i doma používa výhradne Linux a FreeBSD. Hranie a vývoj hier sa venuje vo voľnom čase.

URL článku:

www.linuxexpres.cz/06u2

Hlboko v zlatej ére 8bitových počítačov, keď Amiga 500 bola ešte neznámym pojmom, uviedol tajomný Dr. Sepulveda na trh počítač novej generácie, Protologic 68000. Menšie technické chyby v koncepte však prerástli až do úplného kolapsu celého projektu a namiesto ovládnutia sveta zostal Sepulveda sám so skladmi plnými počítačov.

Potom sa ale stalo niečo zvláštne – jedna z chýb vyvolala v okolitých počítačoch niečo, čo Sepulveda nazval „kvantovou rezonanciou“. Stroje sa spojili do siete, ktorá svojím fungovaním zo všetkého najviac pripomínala ľudský mozog. Doktor vrhol všetky svoje sily do výsledného projektu a vytvoril digitálny zábavný park, obývaný malými zelenými Darwiniánmi, ktorí sa počas tisícok generácií v duchu pravidiel evolúcie vyvinuli na prvú umelú inteligentnú formu života. Vy máte tú česť patriť medzi návštevníkov spomínaného parku.

Ak sa vám zdá, že je príbeh hry Darwinia poriadne strelený, nemýlite sa. Ak sa ale naozaj vydáte do digitálneho sveta obývaného postavičkami z klasických videohier, zistíte, že je nielen zaujímavý, ale aj neuveriteľne zábavný. Chris Delay a Andy Bainbridge z Introversion Software totiž urobili to najlepšie, čo mohli. Prišli s nápadom, zistili aké sú ich možnosti, výhody, ale aj obmedzenia, a potom práve svoje vlastné obmedzenia využili takým spôsobom, aby výslednú hru ešte zlepšili. Ako je to možné?

Darwinia sa podobne ako Uplink (predchádzajúca hra od Introversion) len veľmi ťažko zaraďuje do nejakého žánru, ale keby ste veľmi prosili, väčšina hráčov by sa zrejme nejako zhodla na 3D akčnej realtimovej stratégii. Introversion síce dokázali vytvoriť výkonný engine a kvalitné objekty, ale pri danom počte vývojárov (rozumej 2) by vytváranie fotorealistických textúr, zložitých animácií a automatického prepočítavania pohybu postáv po mape jednoducho zabralo príliš veľa času, ktorý autori radšej venovali odlaďovaniu programu a dôrazu na hrateľnosť.

Téma, ktorú si zvolili, ich zbavila časti problémov. Nielen, že je digitálny svet Darwinie originálny, ale vďaka prítomnosti postáv známych z tých najstarších

hier je pre väčšinu hráčov aj okamžite identifikovateľný (mladší ich poznajú z mobilných telefónov). Jednoducho povedané, nostalgická atmosféra zašlých čias počítačovej zábavy vo vysokom rozlíšení s kvalitnými detailami a pri vysokej rýchlosti (ak nemáte príliš starý systém, uvedené technické požiadavky berte ako minimálne) vám v hre poskytne naozaj estetický zážitok, a to bez nutnosti programovať napríklad mimiku tváre (ktorú digitálne postavičky nemajú).

Druhé obmedzenie sa zdá byť ešte závažnejšie. Len veľmi ťažko môžete hráčom predložiť realtimovú stratégiu v prípade, že sa jeho jednotky nedokážu sami bez problémov presúvať po mape aj na veľké vzdialenosti. V Darwinii je ale práve toto jedna z najväčších devíz hry, keďže nutnosť priameho ovládania vojenských jednotiek je práve to, čo robí väčšinu misií zábavnými (a niekedy aj pomerne zložitými).

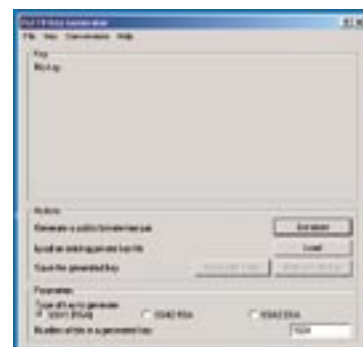
Pýtate sa, čo hľadajú vojenské jednotky v zábavnom parku? Krátko po vašom príchode sa dozviete, že ste vlastne jediný návštevník – park bol kvôli invázii vírovej nákazy uzavretý. Ak chcete pomôcť chudákovi Darwiniánom prežiť a poraziť vírusy, budete sa musieť chopiť ovládania a vyvolať svoju prvú jednotku.

Na tomto mieste by som sa na chvíľu zastavil – pri pôvodnom uvedení hry v marci 2005 sa všetky jednotky v hre, ktoré mimochodom spúšťate ako programy a majú aj príslušné verzie (na rozdiel od praxe zaužívanéj v linuxovom svete začínajú väčšinou od verzie 1.0), vyvolávali kreslením geometrických obrazcov myšou. Originálne riešenie, ale mnohým hráčom zrejme pripadalo zložené. Introversion urobili v komerčnom svete pomerne nevídaný krok a s najnovšou záplatou do hry uviedli aj iný, jednoduchší systém vyvolávania jednotiek prostredníctvom ikon.

Základné jednotky sú v podstate dve: vojenská, ktorá za použitia viacerých zbraní bojuje s vírusmi, a inžinier, ktorý zbiera dušičky mŕtvych vírusov či Darwiniánov, preprogramováva vírusmi obsadené budovy a zbiera stratené prvky výskumu Dr. Sepulveda. Zozbierané dušičky sa potom v budove zvanej inkubátor (ak ju pravda máte) pretvoria na nových obyvateľov digitálneho sveta. V priebehu hry získate

Autentizace pomocí klíčů

Lukáš Zapletal ukáže, jak skoncovat s hesly v programu Putty.



Jistě jste si všimli, že pokud mluvíme o komunikaci protokolem SSH, bavíme se o zabezpečeném kanálu, nikoliv bezpečném. Pokud budete mít komunikaci zabezpečenou sebelepší šifrou a ztratíte lístek se svým heslem, na server se může útočník dostat. Co je ale horší – lidé si vytvářejí snadno zapamatovatelná a často také jednoduše uhádnutelná hesla. A to je největší problém autentizace osob pomocí hesel.

V Linuxu používáme balík OpenSSH obsahující jak SSH server (sshd), tak i klient (ssh). Tato implementace používá asymetrické šifrování RSA pro výměnu komunikačních klíčů a dále symetrické šifry 3DES, Blowfish, AES a Arcfour pro vlastní přenos (RSA je výpočetně náročná šifra, pro vlastní přenos dat jsou vhodnější symetrické šifry). Vše je naprosto transparentní.

Protokol SSH, který OpenSSH implementuje a který vytváří pracovní skupina při IETF, umožňuje autentizovat uživatele pomocí RSA klíčů. V praxi to zkrátka znamená, že při připojování po vás server nechce heslo, ale také veřejný klíč. Server s ním zakóduje bezpečnostní token, a pokud jej klient správně dekoduje (samozřejmě tajným klíčem, který má jen on) a pošle zpět serveru, je vpuštěn do systému.

Mezi hlavní výhody tohoto způsobu ověřování uživatelů je právě absence hesla. Uživatelé si nic nemusejí pamatovat, nic si nepíší na lístečky a nelepí si je na monitor. Ještě větší přínos však vidím v naprostém znemožnění útoku hrubou silou – pokud bude autentizace hesly úplně zakázána.

Jak tedy ve Windows na to? O programu Putty jsme se již zmiňovali (LinuxEXPRES 12/2005). Obsahuje program `puttygen.exe`, kterým si můžete vygenerovat svoji dvojici klíčů. Po klepnutí na tlačítko program požádá o náhodné pohyby myši nad šedou plochou okna (potřebuje vygenerovat dostatečně „dobrá“ náhodná data). Poté budete dotázáni na tzv. `passphrase` – heslo, kterým bude tajný klíč zašifrován.

Asi jste si již uvědomili, že pokud by se někdo zmocnil tajného klíče, mohl by se hlásit na všechny serve-

ry, které by pomocí něj autentizovaly vstup. A jelikož se pohybujeme ve vodách operačního systému Windows (kde „pluje“ spousta spywaru, malwaru a trojanů – ty mají hesla velmi rády), zvolíme dostatečně silné heslo (šest znaků by vám mělo dát dostatečný čas pro změnu klíče po odcizení). Nyní stačí klíče uložit do vámi zvoleného adresáře, nezapomeňte si správně pojmenovat, který je veřejný (public) a který soukromý (private)! V dialogu dole můžete změnit nastavení klíče, já důrazně doporučuji šifru RSA a verzi SSH 1 (pro tu je i tento návod). Délka 1024 bitů je pro účely autentizace dostačující.

A nyní ta legrační část. Veřejný klíč musíte nějakým způsobem dostat na server. Můžete použít SCP (viz minulé číslo LinuxEXPRESu), nebo jej poslat klidně e-mailem. Nemusíte zkrátka použít zabezpečený kanál, protože z veřejného klíče útočník ten tajný nemůže odvodit. Jakmile jej budete mít nakopírovaný na serveru, vytvořte v adresář `~/.ssh`, pokud ještě neexistuje. Do něj nakopírujte veřejný klíč a pojmenujte jej `authorized_keys`. Pokud takový soubor existuje, připojte jej na konec pomocí příkazu `cat muj_klic >> authorized_keys`.

Nyní si na ploše vytvořte zástupce s programem `pageant.exe`, který se rovněž dodává s balíkem putty (musíte si stáhnout ZIP variantu nebo installer, pokud máte jen binárku `putty.exe`). Jako parametr zadejte cestu k soukromému klíči (do uvozovek, pokud máte v cestě mezery). Nyní, když se budete chtít připojovat pomocí klíče, stačí spustit Pageant, ten se zeptá na heslo ke klíči a po zadání se schová do ikonové oblasti. Putty si od něj klíč při spojení vyžádá. Hotovo, nezapomeňte pečlivě zamykat stanici pokaždé, když se od ní jen na chvíli vzdálíte!

V Linuxu si klíče vygenerujete programem `ssh-keygen` (parametr `-t` udává metodu: `rsa1` pro SSH1, `rsa` a `dss` pro SSH2), který je vygeneruje rovnou do adresáře `~/.ssh`, s čímž počítá i klient. Na server pak stačí dopravit soubor `~/.ssh/id_rsa.pub` (eventuálně `dss` při použití tohoto algoritmu) podobným způsobem. Jen připomenu, že pokud použijete protokol SSH2, pak cílový soubor pojmenujte `authorized_keys2`. ■

Pokud se připojujete na server poprvé, klient zobrazí hlášení, že nezná veřejný klíč serveru. Obvykle zobrazí také otisk klíče, tzv. *fingerprint* a vyžaduje explicitní potvrzení („Yes“). Napoprvé tuto hlášku můžete odklepnout, ti otrlejší si mohou poznačit otisk do deníčku. Vždy, když se bude klient znovu připojovat, tak veřejný klíč serveru srovná s tím, který již zná.

Kdykoliv však uvidíte znovu toto hlášení, kontaktujte administrátora serveru. Pakliže vám potvrdí, že s klíči na serveru nic nedělal, buďte velmi obezřetní. Můžete se totiž přihlásit a úplně cizí (podvržený – například změnou DNS záznamu) server. Každý správný administrátor tajný klíč serveru zálohuje a při upgrade systému jej obnoví.

Je velmi důležité, abyste této poznámce na okraji porozuměli, jinak se vystavujete nebezpečí, že si někdo „zahraje na váš server“ (útok *man-in-the-middle*). Zpráva s *fingerprintem* ve vás prostě musí vyvolávat mimořádné podezření.

O autorovi:

Lukáš Zapletal (*1980) se věnuje Linuxu již řadu let, napsal mnoho článků pro internetové magazíny a nyní působí jako šéfredaktor LinuxEXPRESu. Ve volném čase se věnuje elektronické hudbě.

URL článku:

www.linuxexpres.cz/06x2