Slovník a mapy

TOMÁŠ JIRÁSKO

■ Pocket Translator nabízí nejrozsáhlejší slovníkové databáze pro kapesní počítače na trhu, včetně příkladů použití, psané podoby (pouze u angličtiny) i namluvené výslovnosti. Díky pokročilým kompresním algoritmům je možné i největší slovníkové databáze uložit do omezené vnitřní paměti kapesního počítače a přitom stále rychle prohledávat. Vyspělé grafické uživatelské rozhranní podporuje technologii prediktivního psaní, umožňuje pracovat s kapesním počítačem „naležato“, a překvapivě nevyžaduje instalaci lokalizace. Lokalizovaná aplikace SmartMaps obsahuje rastrové mapy a samotný program pro práci s těmito podklady. Program nabízí kompletní instalaci buď na kartu, nebo do RAM PDA (u menších map) a je k dispozici pro Palm OS od verze 4.0 a všechny Pocket PC zařízení. Obdobnou funkčnost nabízí i verze pro Windows. Program umí pracovat s více mapami, mezi nimiž lze snadno přepínat. Na kartě tak lze mít Autoatlas i mapu Prahy a v případě potřeby dokoupit další mapu z aktuální nabídky. Program je prodáván ve společném balení pro obě platformy.

Odkaz: *www.ahmobile.cz*

Tissot s Microsoftem

ČESTMÍR ŽÁK

■ Švýcarský výrobce náramkových hodinek Tissot se rozhodl zařadit do své nabídky produkt High-T Watch s podporou technologie SPOT (Smart Personal Objects Technology) pocházející od Microsoftu. Hodinky High-T Watch disponují dotykovým displejem, na němž si díky spolupráci s MSN Direct můžete mj. přečíst aktuální zprávy či předpověď počasí. Tyto informace jsou do hodinek doručovány prostřednictvím speciálních FM rádiových vln (za poplatek 9,95 USD měsíčně nebo 59,95 USD ročně). Cena High-T Watch činí 725 USD (cca 19 000 Kč), což tento produkt (dokonce i v odlišných finančních poměrech, jež panují v USA) předurčuje k prodeji pouze v obchodech s luxusním zbožím. Přesto si Microsoft nově vzniklou spolupráci velice pochvaluje a doufá, že bude možné s produktem již brzy expandovat do Evropy.

Odkaz: *www.tissot.ch*

Systémy prevence neoprávněného průniku

V minulém čísle PC WORLDu jsme se věnovali systémům detekce neoprávněného průniku (Intrusion Detection System, IDS), dnes se budeme věnovat systémům prevence těchto neoprávněných průniků (Intrusion Prevention System, IPS).

V současné době se již za adekvátní ochranu vnitřní sítě nepovažuje pouze router v součinnosti s firewallem. Komplexní zabezpečení se nyní skládá z výše zmíněných zařízení a následně pak také z dobře distribuovaných instalací nových bezpečnostních záplat, datových vzorků antivirových produktů a dalších bezpečnostních balíčků pro používané aplikace. Dnešní administrátor pak musí stále více řešit problémy se správným zabezpečením celé sítě z hlediska vnějšího napadení ať už na úrovni zmíněného firewallu, či na úrovni dalších zařízení, které umožňují přístup do vnitřní sítě (jako bezdrátové přístupové body a další zařízení).

V minulosti se dbalo právě na zabezpečení vstupních bran, a proto se změnily i techniky průniku do sítí, případně technika krádeží dat či kompromitace jednotlivých serverů a stanic. Nyní lze s velkou mírou pravděpodobnosti říci, že útoky jsou častěji vedeny tzv. z vnitřní strany, a proto se hůře odhalují. Proto (a nejen proto) se nyní doporučuje využívat zařízení, které monitoruje toky dat v DMZ, v kritických lokalitách, popř. v celé vnitřní síti. To pak obstarávají systémy IDS. Nová generace těchto zařízení umožňuje nejen monitoring, ale i následnou akci v reálném čase – tyto systémy označujeme právě IPS.

Základním rozdílem mezi IPS a ostatními ochrannými prvky je proaktivní přístup k informační bezpečnosti. Zatímco běžné firewally dokáží provoz pouze blokovat či propouštět, systémy IPS v tomto provozu umí nalézt škodlivé kódy a rozpoznat pokusy o útok. Zatímco běžné detekční metody vydají v případě nebezpečné situace pouze varování a čekají na akci či pokyn k akci od uživatele/administrátora, systémy IPS okamžitě přijímají odpovídající protiopatření (podle nastavené bezpečnostní politiky), aby útok zhatily už v počátku.

Některé systémy IDS sice mají určité obranné mechanismy implementovány také (ukončení TCP spojení, rekonfigurace firewallu po zjištění útoku aj.), ale ty zpravidla nejsou schopné reagovat s dostatečnou rychlostí, protože mezi detekcí útoku a pokusem o jeho zblokování uplyne krátká, leč významná doba. Naproti tomu systémy IPS nepoužívají k likvidaci útoků žádné další prostředky, ale s nebezpečným paketem nebo spojením se vypořádají okamžitě.

K základním úkolům systémů IPS patří:

- Identifikovat neautorizovaný provoz založený na signaturových vzorcích.
- Identifikovat neautorizovaný provoz založený na detekci anomálií v protokolech.
- Ukončit nebo znesnadnit služby spojené s nežádoucí činností.
- Logovat všechny monitorované činnosti.
- Zajišťovat důkazy o nepřátelské činnosti v anomálních paketech.

Rozlišujeme přitom systémy IPS dvojího typu – uživatelské a síťové. Zatímco uživatelské jsou instalovány na lokálních stanicích a chrání je před jednotlivými útoky, síťové mají na starosti veškerý provoz příchozí zvenčí. Oba typy přitom mají své výhody i nevýhody. Zatímco uživatelské IPS je velmi pevně spjato s konkrétním operačním systémem a jeho upgrade může působit potíže, u síťového je zase obtížné zajistit, aby v dnešní době bezdrátových, mobilních a jiných připojení k síti šel skutečně veškerý provoz přes tento systém (jinak IPS samozřejmě pozbývá smysl).

Systémy prevence neoprávněného průniku tak představují další stupeň k zajištění bezpečnosti informačních technologií před útokem zvenčí.

TOMÁŠ PŘIBYL, AEC
www.aec.cz