"Velký bratr"

V boji proti virům a pirátským kopiím se Microsoft a spol. chystá k velkému útoku: monitorovací čipy, povinná registrace a ochrana proti kopírování mají z každého PC vybudovat domácí pevnost. Cena za tuto bezpečnost je však vysoká: hrozí totální kontrola. Chip ukazuje, co vše se na uživatele chystá.

" Velký bratr" přichází potichu. V pochmurných vizích budoucnosti od Orwella, Huxleyho a spol. to byl ještě všudypřítomný stát, který své občany sledoval na každém kroku. Dvacet let po "1984" vypadají scénáře kontrol a jejich protagonisté jinak: globálně agitující průmyslové a obchodní koncerny si vymýšlejí stále rafinovanější metody, aby ve jménu bezpečnosti mohly kontrolovat, rozdělovat a analyzovat své zákazníky. Ještě nikdy nebylo tolik různých možností pro tajné špehování jako nyní.

Za novými technikami kontrol stojí slova jako Next Generation Secure Computing Base (NGSCB), Digitals Rights Management (DRM) nebo Radio Frequency Identification (RFID). Že tomu nerozumíte? Právě to je také účelem. Prominentním podporovatelem všech těchto technik je Microsoft. Koncern svázal internet tak pevně s Windows, že uživatelé stěží poznají, kdy je jejich systém v kontaktu s Redmondem. Ale to byl teprve začátek. V nových koncepcích, jako je Trusted Computing, vidí kritici počátek rozhodující etapy na cestě ke zbavení uživatelů PC svéprávnosti.

Nové náměty mohou skutečně zajistit větší bezpečnost. Ale kdo by se necítil stísněně, když jsou jeho data v rukách několika málo firem? Nahlédněme společně za kulisy hezkého nového světa IT a snažme se být nezaujatí. Vysvětlíme vám, jak fungují nové techniky - a jaká nebezpečí skrývají.

Microsoft
TCG: Bezpečnostní kartel

Aliance nejvýznamnějších světových IT firem chce pomocí hardwaru a softwaru vybudovat z PC pevnost. Permanentní kontroly by měly odradit hackery, viry a pirátské kopie. Problém: Kdo kontroluje kontrolory?

Jak si představujete absolutně bezpečný PC? Počítač, na který nemají přístup hackeři a viry a na který nelze nainstalovat žádný chybný ovladač? Zní to dobře. Přesně toho chce docílit strategie Trusted Computing Group (TCG) - a chce toho docílit dokonce ještě více: úkolem TCG je vyvinout otevřené bezpečnostní standardy pro PC, notebooky, PDA, mobilní telefony a všechny myslitelné druhy speciálních počítačů, např. peněžní automaty. Vedení skupiny, hodlající zavést novou bezpečnostní strategii, představují skutečné špičky IT průmyslu: AMD, HP, Intel, Microsoft, Sony a Sun tvoří nejvlivnější kruh, tzv. "Promoters". Platí za to v porovnání skromných 50 000 dolarů za rok. O stupínek níže v této hierarchii jsou "Contributers". Za 15 000 dolarů ročně smějí mít v pracovních skupinách vliv na technické specifikace. Tento status mají firmy jako ATI, Fujitsu-Siemens, Nokia, nVidia, Philips a Samsung. Docela dole jsou "Adopters". Jsou to firmy jako AMI, Gateway a Toshiba, které smějí za 7500 dolarů testovat vývoj TCG v beta stadiu. Poplatek se zdá být nízký, ale pro soukromé softwarové firmičky nebo malé open source projekty je i 7500 dolarů příliš. Důsledek - zůstávají mimo.

Srdcem konceptu TCG je čip na základní desce: Trusted Platform Module (TPM), přezdívaný jako čip Fritz, pojmenovaný po americkém senátorovi Fritzovi, který se hodně angažoval v zavádění kryptografie. Tento čip funguje již při bootování systému jako určitý druh hardwarového klíče (dongle), pro kompletní kontrolu však ještě potřebuje softwarovou podporu. A hle: Microsoft je již s Next Generation Secure Computing Base (NGSCB) připraven ve startovních blocích.

Trusted Computing (TC) zní dobře - kdo by také měl něco proti důvěryhodným PC? Zejména když budou hlavně ve firmách, které tím získají konečně čisté sítě - sen administrátorů. TCG chce zavést logo, které si každý výrobce, jehož hardware bude kompatibilní s TCG, bude smět vytisknout na svůj obal. To, zda výrobek splňuje požadavky, mají přezkušovat nezávislé instituce. Bez certifikátu pak nebude fungovat ani software, ani hardware, pokud si to administrátor nebude přát.

KONTROLA: BEZ LICENCE A AKTIVACE NEJDE NIC

Certifikace a přezkoušení nezávislými organizacemi na národní úrovni by vzaly kritikům vítr z plachet. Ti se však obávají, že by se TCG mohla vyšplhat až na globální superinstanci, která bude sama rozhodovat, které výrobky jsou důvěryhodné. TCG však bude certifikovat pouze čip Fritz jako jádro celé

věci. Funguje to takto: Pokud uživatel čip zapne (standardně je tato součástka vypnutá), vytvoří se v procesu zavádění systému kontrolní součet (Hashcode), který shrne, které komponenty hardwaru jsou v PC zabudované. Na základě těchto hodnot rozpozná TPM, zda např. BIOS hlavní desky je ve stavu, v jakém byl původně dodán.

Důležité: Čip je pasivní součástí, tím pádem není schopen blokovat hardware nebo software. Ukládá například kontrolní součet hardwarových součástí, použité klíče v systému nebo bezpečnostní certifikáty. Uživatel nebo administrátor jsou vždy svázáni se všemi kroky a dávají poslední rozhodnutí. Pokud čip Fritz na základě zkušebního součtu zjistí, že některá hardwarová součást není certifikovaná (a je tedy "nedůvěryhodná"), sdělí to uživateli. Je-li však uživatel přesvědčen, že součástka je "čistá", může dát "zelenou". TPM potom uloží tento stav PC jako "důvěryhodný".

Čip Fritz není důležitý jen proto, aby ochránil hardwarovou konfiguraci systému proti zásahům zvenčí. V běžícím provozu sleduje, aby na PC nebyl spuštěn software, který není certifikovaný - např. viry.

K tomu potřebuje operační systém, který umí využít schopností TPM. A tady již vstupuje do hry Microsoft. V dalším operačním systému Longhorn, který se objeví pravděpodobně v roce 2006, bude integrována technologie NGSCB. Podle vyjádření zástupců Microsoftu bude NGSCB standardně vypnutá. Navíc by tak postupovali i veškeří OEM partneři softwarového gigantu.

Aby uživatel vůbec mohl systém s aktivovanou technologií NGSCB obsluhovat, musí nejdříve podstoupit autentifikaci. To lze učinit například prostřednictvím klávesnice konformní s NGSCB, protože také vstupy a výstupy počítače bude technika sledovat. (Jinak, než je tomu u dosavadních Windows, kde každý hardware a každý program komunikují se systémem a tak mohou neomezeně přistupovat do pracovní paměti a na pevný disk). Počítač s NGSCB bude rozdělen na dvě oblasti: nechráněnou, ve které bude vše fungovat jako doposud, a chráněnou, ve které bude veškerá komunikace probíhat přes zkušební instanci, tzv. Nexus (viz rámeček str. 28).

Při instalaci nového softwaru předá TPM do klíčového serveru na internetu kód, vytvořený ze sériového čísla programu a kontrolního čísla PC (Hashcodu). Server odpoví aktivací programu a uloží data počítače na webu.

Důsledek: Software je nyní pevně svázán s počítačem, okamžitě lze vysledovat, když je například jako pirátská kopie instalován na jiném systému. Viry zůstávají mimo, protože každý program, který je používán pod NGSCB, musí projít aktivační rutinou.

Nexus tedy přezkušuje každý dotaz na systém, zda je důvěryhodný. Potřebné informace jsou v zakódovaném stavu uloženy v čipu Fritz. Když například Media Player požaduje přístup do pracovní paměti, Nexus otestuje, zda je tento nástroj Microsoftu stejně jako předtím v čistém stavu.

Komunikaci mezi Nexusem a instalovaným softwarem zajišťují "agenti"; přenášejí sem a tam klíče a certifikáty, které si předtím vyzvedli z TPM. Na úrovni hardwaru TPM navíc kontroluje, zda jsou například monitor, myš, grafická karta a USB skener důvěryhodné - jsou jen tehdy, když umějí zpracovávat zakódovaná data. To má za následek, že když chce někdo provozovat svůj počítač s NGSCB, potřebuje kompletně nový hardware. (Ochranný software má jednoduše nové požadavky na hardware.) Koncept Microsoftu Secure I/O, tedy koncept bezpečných vstupů a výstupů, neznamená nakonec nic jiného, než že všechna data, která se dostávají do PC přes vstupní zařízení, jako je klávesnice nebo myš, a všechna data, která jsou přes grafickou kartu vydávána na monitor, budou posílána zakódovaná. Data kóduje čip TPM, délka klíče je v současné době 2048 bitů.

MŮŽE SE UŽIVATEL SVOBODNĚ ROZHODNOUT? INTEL TRVÁ NA POVINNÉ KONTROLE

Uživateli má tedy zůstat možnost volby, zda si přeje systém chráněný pomocí čipu Fritz a NGSCB, nebo zda bude používat Longhorn jako své dosavadní Windows. Jedno je jisté - pokud zůstane bezpečnostní systém Microsoftu deaktivovaný, nemůže být pod Windows používán ani TPM. V tomto bodě si odporují plány člena TCG Intelu a Microsoftu, protože výrobce čipu trvá na tom, aby byla technologie NGSCB aktivována vždy - není se co divit, když se na tom dá pěkně vydělat. Proto Intel již nyní plánuje, že bude do budoucích strojů integrovat vlastní hardwarovou variantu NGSCB s názvem La Grande.

Ani Microsoft nepropaguje NGSCB jen z lásky k bližnímu. Jeho image trpí stále nově objevovanými bezpečnostními mezerami; s NGSCB by mohl koncern zahájit generální útok proti hackerům, virům a nezabezpečeným ovladačům. Uživatel má mít jistotu, že jeho počítač je imunní proti zásahům zvenčí. Základní rys bezpečnostní architektury označují zástupci Microsoftu jako "magický trojúhelník", tvořený autentičností uživatele, strategií Content Security (jasná pravidla pro přístupová práva k obsahům) a integritou stroje. Posledně jmenovaná integrita stroje má zaručit, že se do systému budou moci instalovat jen "čisté" programy. Již teď si Windows XP stěžují na ovladače, které nebyly testovány Microsoftem, nicméně po jednom kliknutí myší odkaz zmizí - to se však má brzy změnit.

Kromě bezpečnostního aspektu jde tedy o peníze. To platí hlavně pro prodejce softwaru. Ti jásají, protože možnosti použití pirátských kopií se značně omezí. NGSCB totiž umožní to, že každý program bude kryptograficky aktivován přes web - cracky a hackeři zde nemají šanci.

U open source softwaru se však tato forma kontroly může projevit ničivě. Minimálně v prostředí NGSCB nesmějí tyto programy běžet. Microsoft přesto tvrdí, že koncern dá programátorům bezplatného softwaru zdarma k dispozici Software Development Kit (SDK), aby tak mohl každý vytvářet své nástroje kompatibilní s NGSCB. Také Hewlett-Packard nasadil smířlivý tón: jeho vývojáři svolali v říjnu minulého roku obec "open source", aby se účastnila na vývoji Trusted Computing. O minimálních 7500 dolarech za vstup do TCG však nebyla řeč.

Východiskem z dilematu open source nebo freewaru by mohlo být rozdělení PC na dvě části, které by NGSCB měla uživateli umožnit. Programy jako MS Office běží v chráněném Nexusu, freeware pracuje paralelně v nechráněném prostoru. Toto řešení zní příliš hezky na to, aby bylo uskutečnitelné. Také není - protože program je sice prostřednictvím Development Kitu kompatibilní s NGSCB, od ní však ještě nemá žádný certifikát. Ten potřebuje nejpozději tehdy, když certifikované obsahy (jako dokumenty nebo videa) vyžadují pro své přehrávání rovněž certifikovaný software - sbohem freeware. Toto svolení by si totiž musel programátor nejprve za poplatek vyžádat u příslušné nezávislé národní instituce. A to zatím opravdu zní jako hudba budoucnosti.

Další problém: Kdo má svrchovanost nad klíči a certifikáty v čipu Fritz? Výrobce softwaru, který uvolňuje program? Sám uživatel? Nadřazená instance, která kontroluje, aby nebyl žádný klíč vydán dvakrát, a která musí kromě majitele znát všechny klíče?

PAMĚŤ PRO UKLÁDÁNÍ KLÍČŮ: STANE SE TPM PRO UŽIVATELE ČERNOU SKŘÍŇKOU?

Nejrůznější uživatelské instituce důrazně požadují, aby kontrola klíčů byla v moci uživatele. Jinak se vlastní počítač stane černou skříňkou, ke které nemá majitel žádný výhradní přístup. V Evropské unii se v uvedeném problému angažují i politici. Například německá spolková ministryně spravedlnosti Brigitta Zypriesová na loňské výstavě Systems uvedla: "Uživatelé musí mít plnou kontrolu nad všemi daty, nezávisle na tom, zda jsou zakódována nebo ne. Nesmí dojít k závislosti na třetí osobě."

Také výrobci hardwaru musí v souvislosti s NGSCB rozlousknout tvrdý oříšek. Počítač s TPM a NGSCB potřebuje sadu čipů a procesor, které mohou stále přepínat mezi jednotlivými režimy. Příklad: Přiřazování paměťových oblastí doposud přebírá operační systém. Platformy jako Linux nebo Windows XP přitom již ale také mají virtuální adresování, u kterého žádný program neví, pod kterou adresou v paměti je provozován. Pouze operační systém má nad tím ještě kontrolu; a to se dá hackovat. Jinak je tomu u NGSCB. Tady musí procesor a čipová sada převzít a řídit adresaci paměti. Pokud přijde dotaz z bezpečného Nexusu, musí se CPU nejprve zeptat TPM, zda je dotaz oprávněný. Když požaduje program z nechráněné oblasti přístup do paměti, vymaže CPU z bezpečnostních důvodů nejprve svoji vyrovnávací paměť a teprve poté přiřadí softwaru adresu v paměti. Každé rozhodnutí procesoru musí odsouhlasit TPM. Kdy budou k dispozici čipové sady a procesory, které jsou k tomu potřebné, je ve hvězdách.

NGSCB PRO SOUKROMÉ UŽIVATELE: VIRY JSOU NEJLEPŠÍM ARGUMENTEM PRŮMYSLU

TCG nestanovuje, kdy si má TPM najít cestu do počítačů. Nabídka se bude zprvu omezovat na firemní oblast, protože tato technika je zajímavá především pro administrátory a firemní sítě. Ti mají oprávněné důvody chránit své počítače před nedovolenými přístupy. Prostor nechráněný NGSCB by byl přitom pro administrátory bezvýznamný.

Soukromí uživatelé se nemohou pro jištěný režim příliš nadchnout, protože by například nemohli spouštět vlastní programy. A před viry je přece chrání software. Navíc nechráněný režim nabízí i nadále prostředí x86 se všemi riziky. Soukromí uživatelé také jen zřídkakdy přijdou do styku s tak citlivými daty, aby potřebovali bezpečný Nexus - kromě on-line bankovnictví a on-line nákupů. Při on-line bankovnictví určitě stačí systém čipových karet HBCI. Jako pouhá náhrada HBCI by byla technologie NGSCB trochu příliš.

Pro tvůrce webového obsahu se naopak nabízí zajímavá možnost použití, protože kromě certifikovaného softwaru se dá s TPM spojit i Digital Rights Management (viz rámeček str. 32). Při on-line koupi hudební skladby by se obchod například nejprve dotázal na hardwarový klíč uložený v TPM počítače kupujícího a zapsal by ho do prodávaného souboru. Tím by bylo možno tuto hudební skladbu přehrávat jen na daném počítači.

I samotný Microsoft se může pomocí čipu Fritz efektivně chránit před piráty. Koncern vlastní více patentů na spojení operačního systému, Digital Rights Management a TPM. Nejpozději při instalaci updatu Windows staženého z internetu by mohl počítač zaslat do Redmondu údaje, jako je jméno a adresa uživatele.

Závěr: Trusted Computing slibuje hodně - žádné viry, žádné pirátské kopie, žádní hackeři. Za to je však nutné přenechat kontrolu nad svým vlastním počítačem velké firmě nebo kartelu. Ne, plány TCG jsou ještě nezralé a neprůhledné. Uživatel rozhodně musí být správcem svého klíče. Pak by ale zase byl koncept bezpečnosti absurdní - je to prostě dilema.

JAK FUNGUJE NEXT GENERATION SECURE COMPUTING BASE (NGSCB)

MODEL MICROSOFTU: BEZPEČNOST V ROZDĚLENÉM POČÍTAČI

Software: Operační systém Longhorn má počítač rozdělit na dvě od sebe oddělené části: na nechráněnou oblast a na chráněnou oblast, která bude řízena NGSCB. V ní poběží jen programy kompatibilní s NGSCB. Na rozdíl od současného stavu nebudou mít tyto programy přímý přístup do pracovní paměti PC, ale s hardwarem budou komunikovat výhradně přes NGSCB. Tato komunikace je jištěna pomocí kódování RSA - 2048 bitů.

Nexus: Stěžejní součástí NGSCB je NexusMgr.SYS. Tento soubor slouží jako záchytná komora pro interní komunikaci počítače. K jeho úkolům patří mimo jiné přiřazování rezervovaných oblastí pracovní paměti jednotlivým programům. Požaduje-li software přístup do paměti, spustí se zakódovaný dotaz na Nexus. Agenti soubory zprostředkují potřebné certifikáty a klíče. Nexus srovná klíč s 2048bitovým klíčem, který je uložen v TPM, a odkáže program na určitou oblast paměti.

Hardware: Na základní desce se nachází TPM. Slouží jako server pro všechny používané klíče. Dokonce i periferní zařízení, jako je klávesnice, myš nebo monitor, komunikují s počítačem v bezpečnostním režimu pouze kódovaně. Čipová sada a CPU stále přepínají mezi NGSCB a "normálním" režimem. Výsledek: Dva počítače v jednom krytu. Nechráněnou oblast lze obsluhovat i s původním hardwarem.

DRM: Totální kontrola

Hudební průmysl má problémy s tím, jak prodávat hudbu prostřednictvím internetu. Důvod: V případě, že se objeví pirátské kopie, musí být možné vysledovat, kdo danou skladbu kdy koupil. Potřebná technika již existuje: Digital Rights Management.

Carmine Caridi je herec. Není sice příliš známý, ale vždy sedí v 5803členné komisi pro udílení Oscarů. Tento devětašedesátiletý herec hrál v mafiánském eposu Kmotr II. Metody zlých chlapů na něm musely zanechat stopy, protože Caridi porušil pravidla Academy of Motion Picture Arts and Sciences: půjčil známému film kandidující na Oscara Po čem srdce touží, který dostal k nahlédnutí, a ten ho dal promptně na internet. Caridiho smůlou bylo, že film na jeho DVD byl opatřen digitálním vodoznakem, který ho v DivX kopii identifikoval jako majitele disku.

Tyto vodoznaky jsou nejmírnější formou Digital Rights Managementu (DRM) a jsou "neviditelně" nanášeny pomocí steganografie do jednotlivých obrazových pixelů nebo zvukových frekvencí. Vodoznak může obsahovat kompletní soubor nebo pouze jednoduché údaje o kupujícím hudebního nebo filmového kusu. Bez této digitální správy práv se neobejde žádná hudební služba. Datové formáty jako Microsoft WMA nebo WMV toho však dovolují ještě více: zakódování, stanovení doby používání nebo počtu uživatelů. Všechny DRM metody mají ale jedno společné: na zákazníka se nepohlíží jako na poctivce, ale jako na potenciálního zloděje.

Německá internetová videotéka T-Online (T-Vision) například vydává licence, které vyprší již za 24 hodin. T-Online přitom používá Microsoft Windows Media Codec 9. Jeho integrovaný Windows Media Rights Management se stará o to, aby nebylo možné filmy po uplynutí 24hodinové lhůty přehrát, zejména tehdy, když už byly znovu uloženy. U live-streams, kterým se vysílají přes internet například koncerty, používá Microsoft Live DRM (viz rámeček na této straně). Výhoda pro prodejce: Obsah nemůže být zachycen předtím, než přijde k zákazníkovi. Nevýhoda pro uživatele: Soubory umí přehrávat jen Windows Media Player 9, alternativní přehrávače jsou mimo. U Media Playeru 9 je praktická jeho funkce zálohování, která jistí získané licence v případě pádu systému.

Jinou cestou, než jsou restriktivní metody DRM, je takzvaný Light Weight Digital Rights Management (LWDRM), kdy má být digitální obsah neomezeně použitelný, ale informace o kupujícím mají zamezit, aby byl soubor nabízen na výměnných burzách. Jestliže hudební portál informuje o tom, že soubory jsou

opatřeny DRM, jen hlupák by tyto písně nabízel na výměnných burzách. Některé downloadové služby ve světě již s LWDRM pracují:

Popfile (Německo): Ve vodoznaku souborů MP3 není jméno kupujícího - není to dovoleno z důvodů ochrany dat -, ale číslo transakce. Vodoznak je tak robustní, že může být přečten i po vypálení písně na CD. Popfile však prý nezastává žádnou tvrdou linii.

Weblisten.com (Španělsko): Tato platforma nabízí hudbu ve formátech WMA a MP3. Soubory MP3 jsou vydávány s vodoznakem, který obsahuje informace o kupujícím. Soubory WMA však přicházejí na PC podle vyjádření prodejců bez vodoznaků a DRM.

Restriktivněji postupují tito hudební prodejci:

Musicload (Německo): Služba se řídí přísnějšími pravidly. Skladby ve formátu WMA sice smějí být přehrávány na PC libovolně často, ale vypáleny mohou být jen jednou až třikrát.

iTunes (USA): Nejpopulárnější platforma sází přirozeně na DRM a není přitom tak štědrá jako Popfile nebo Weblisten. AAC soubory smějí být přehrány na jednom až třech přehrávačích - buď na iPod, nebo na jiných počítačích - a jako audio CD mohou být vypáleny libovolně často. DRM obsahuje údaje o kupujícím, aby se znemožnilo nedovolené šíření. Vypadá to, že Apple našel zlatou střední cestu: hudební kusy s DRM lze sice pomocí iTunes softwaru přes síť přehrát, ale ne zkopírovat. DRM navíc opatřuje hudební soubory klíčem, který se skládá ze sériového čísla pevného disku, z verze BIOS, názvu CPU a produktového čísla (Product-ID) Windows. Kdyby měl být soubor přehrán na jiném PC, zkouší tamější iTunes Player, zda se klíč hudebního souboru hodí k hardwaru.

DRM není zajímavý jen pro oblast zábavy. I v běžném pracovním životě se může používat zadávání práv. Protože vedle hudby nebo videa mohou údaje DRM obsahovat například i e-maily. Obchodní e-mail tak může být určen jen určitému okruhu čtenářů. Zejména formulace "Tato zpráva se sama do 30 vteřin zničí" již není s DRM žádnou vizí budoucnosti.

Závěr: Majitel práv by přirozeně měl chránit své zboží před pirátskými kopiemi. Není však únosné, aby byl on-line kupující již předem podezříván z pirátských úmyslů a zakoupený soubor by směl používat jen omezeně, zatímco ten, kdo si koupí CD, ho může kopírovat libovolně často.

RFID - čip pro všechny případy

Technika kontroly Radio Frequency Identification umožňuje, aby byly informace schovány v etiketách, v oblečení nebo pod kůží. Čipy jsou tenoučké a nepostřehnutelné. Ale kdo má přístup k datům?

" Máte zákaz vstupu na stadion" - takto může skončit návštěva zápasu Mistrovství světa ve fotbale 2006 v Německu ještě před branami stadionu. Důvod: Lístky budou opatřeny RFID čipy. Organizátoři tak chtějí zamezit černému obchodu a falšování.

Hlavním zdrojem prodeje lístků má být internet, platit se bude kreditními kartami. Kdo si chce koupit lístek, musí se nejdříve zaregistrovat u Německého fotbalového svazu (DFB). Svaz nevylučuje, že ihned porovná údaje s databází sportovních násilníků. Jaká data budou na čipu uložena, ještě není zcela jasné. Každopádně se na datový nosič vejde asi jeden kilobajt dat.

Příští MS ve fotbale je ještě vzdálené - RFID už ale ne. Obchodní řetězec Metro (u nás Makro) používá tuto techniku od roku 2003 ve svém "Future Store" v Rheinbergu. Jiskřící cenovky tam slouží především k ochraně před krádežemi: když se RFID dostane za bezpečnostní uzávěru, spustí se alarm.

Technicky není RFID žádný velký vynález: čipy nepotřebují žádné vlastní zdroje energie - jsou aktivovány při čtení pomocí elektromagnetického impulzu čtecího zařízení. V případě lístků na MS smí být vzdálenost od čtecího zařízení deset až dvanáct centimetrů, v případě jiného použití může být i větší.

Jak jednoduché je použití techniky RFID, tak velké jsou možnosti jejího zneužití. Když opouštíte obchod, tlačíte nákupní vozík přes elektronickou závoru, která pošle impulz do směru etiket. Čipy nahlásí cenu na pokladnu, částka se automaticky odečte z vašeho účtu. V pozadí se sbíhají všechny údaje do výpočetního střediska, jsou vyhodnocovány a je z nich sestaven profil kupujícího. Ve spojení s vašimi osobními daty by bylo vaše nákupní chování otevřenou knihou. Teoreticky je to možné, v praxi je to však ještě příliš drahé. Bude trvat ještě 10 až 15 let, než k tomu dojde. Důvod: Čipy RFID se nedají ze všeho stejně přečíst, protože sklenice se zeleninou, sáčky s mlékem a mražené zboží různě odrážejí paprsky čtecího zařízení. Kromě toho zatím nemá smysl vybavit jogurt za 10 korun čipem za 12 korun. Čím více čipů se však bude vyrábět, tím budou levnější.

Ochránci dat v EU sledují vývoj ostražitým pohledem.

Závěr: Vše je na zákonodárcích. Ti by se měli postarat o to, aby nikdo nezacházel hanebně s nashromážděnými daty. Informace vztahující se k osobám nemají na čipech co hledat. Pro obaly s RFID by měla platit obecná označovací povinnost. Etikety musí být zničeny, jakmile zákazník opustí obchod. Kdo je extrémně nedůvěřivý, může jít ještě dále: před prvním oblečením může vložit své nové džínsy do mikrovlnné trouby - její paprsky totiž čipy RFID zničí.

Pilní sběratelé dat

Windows XP jsou pověstné svým zjišťováním zákaznických dat. Ale cenná data se sbírají nejen skrytě. Systémy Rabatt sázejí na dobrovolnou spolupráci svých zákazníků.

" Dobrý den, pane Nováku," zdraví on-line knižní obchod. Ale jak ví, že na webové stránce právě surfuje pan Novák, a ne paní Novotná? Je to docela jednoduché: po první objednávce uloží obchod jméno do cookie na zákazníkově počítači. Když se zákazník dostane na první stranu on-line obchodu, dotáže se obchodník cookies a tak zjistí, s kým má tu čest.

Webový prohlížeč od Microsoftu se navíc doposud vůbec nesnažil tuto praxi znemožnit. Alespoň že Internet Explorer 6 má konečně Cookie Management, pomocí kterého se dají tyto malé soubory lépe řídit a mazat.

Ale prohlížeč nevypouští informace do webu jen přes cookies. V menu Internet Options nabízí IE možnost zobrazit příbuzné linky na webové stránky. Získáte tak sice více informací o jednom tématu, ale potřebujete k tomu aktivní plug-in firmy Alexa (dceřiná firma Amazon.com). Tento plug-in vás vede k příbuzným stránkám - a vytváří tak profil vašeho chování při hledání na internetu. Ale to ještě není všechno. Se zavedením Windows XP propojil Microsoft operační systém s webem tak, že často není jasné, kdy jsou kam posílány informace.

Ne nadarmo patří nástroj XP Antispy k povinnému vybavení každého počítače s Windows XP. Obávané "infiltrační" funkce se dají tímto nástrojem vypnout. Do toho jsou zahrnuty i neškodné funkce, jako je nastavování hodin, ale také závadné, jako je chybová zpráva, při které se Microsoftu rovněž pošle vyobrazení pracovní paměti.

Největší ždímačkou dat je však Media Player. Posílá seznamy přehrávání a použité kodeky ven na web. Kontaktuje rovněž Redmond, jakmile se do mechaniky vloží audio CD. Nerozhoduje, co si přehrávačem nastavíte, nejprve se vytvoří spojení. Laici mají často dojem, že software v režimu off-line vůbec nefunguje. Dalším fíglem Microsoftu pro získání informací jsou smart tagy. Ty jsou sice velmi užitečné, mohou dát po kliknutí pravým tlačítkem vysvětlení k určitému pojmu, kliknutí na jedno slovo vás však dovede do on-line encyklopedie Encarta Microsoftu - a opět jdou všechny informace do Redmondu. Je sice nepravděpodobné, že by koncern skutečně vyhodnocoval údaje od milionů zákazníků, ale uměl by to a vy na to nejste upozorněni.

Microsoft pravděpodobně nesestavuje profily, ale obchody na internetu od toho nejsou daleko, a to včetně takových obrů, jako je Amazon.

Není žádný důvod pochybovat o dodržování práv Amazonem. Přesto přináší používání osobních služeb rizika, jak ukazuje případ z října 2003. Mladá Němka chtěla cestovat za svým snoubencem do USA. Po příletu do Atlanty byla zadržena. Na dotaz po důvodu dostala překvapující odpověď: úředník na hranicích zjistil u Amazon.com, že prý má zálibu v "podezřelé literatuře". Podle tiskové mluvčí Amazon Deutschland šlo skutečně o nahlédnutí do seznamu přání té paní. Do toho však může volně nahlížet kdokoliv. Proto se vyplatí i při obyčejném brouzdání na internetu hodně přemýšlet.

Závěr: Kdo dá souhlas ke sběru vlastních dat, je si sám vinen. Přesto musí být jasné, kdo data dostane; a vždy musí být možnost zrušení. V USA sestavují reklamní firmy profily a bombardují potenciální zákazníky dopisy, telefonáty nebo e-maily. Ve srovnání s tím žijeme v Česku (a i v celé EU) na ostrově blaženosti - zatím.

Stefan Reinke

SOFTWARE

BEZ VAŠICH ÚDAJŮ NIC NECHODÍ

S Office a Windows XP to začalo: Microsoft požadoval aktivaci softwaru přes internet. Jiní výrobci ho následovali - a jdou v jistém ohledu ještě dále: nutí kupující svých programů, aby se nechali zaregistrovat zadáním svého jména a adresy.

Nucená aktivace

Microsoft Windows XP
Microsoft Office XP
Adobe Photoshop CS
Cute FTP
Digimap pro Palm
Tomtom Navigator

Update jen po registraci

Panda Antivirus Platinum
Powerquest Partition Magic
Powerquest Drive Image
Microsoft Office XP

DIGITAL RIGHTS MANAGEMENT

JAK FUNGUJE DRM U MICROSOFT MEDIA PLAYERU 9

Služby typu Video-on-Demand (např. německá videotéka T-Vision) vysílají pro zákazníky filmy přes internet. Aby se zabránilo nedovoleným kopiím, jsou videa opatřena Digital Rights Managementem. Výsledkem je, že po 24 hodinách jsou filmy nepoužitelné. Stejná metoda se dá použít také u live-streams v reálném čase.

1. Prodejce

Server prodejce dává k dispozici soubor požadovaný zákazníky, opatří jej informacemi DRM, jako je datum expirace a oprávnění k použití, a zakóduje je. Vytvoří se licenční klíč.

2. Internet

A Soubor je připraven na webovém serveru prodejce k downloadu nebo streamingu.
B Klíč, který umí soubor znova rozkódovat, se uloží na externí licenční server.

3. Uživatel

Media Player stáhne nebo spolu s proudovým formátem obdrží soubor z webu. DRM mu sdělí, kde najde příslušný klíč. Player poté kontaktuje licenční server a obdrží klíč. Následně může být soubor přehrán.

JAK FUNGUJE RFID

CHYTRÉ ETIKETY NA OBALECH

Napájení a informace pomocí rádia:

Když se čipy RFID dostanou do dosahu čtecího zařízení, přenášejí své informace (až 64 Kb) pomocí rádiových vln (do vzdálenosti přibližně pěti metrů). Potřebnou energii si vezmou pomocí antény z elektromagnetického pole, které je vytvořeno čtecím zařízením. Protože čipy tímto způsobem pracují bez baterie, hodí se jako cenovky. Anténa RFID-Chip

1. Dotaz

Čtecí zařízení vyšle elektromagnetický aktivační impulz na etiketu s čipem RFID.

2. Odpověď

Etiketa (čip RFID) využije energii aktivačního impulzu, aby poslala svá data ke čtecímu zařízení.

3. Zpracování

Čtecí zařízení pošle data dále na počítač. Ten data nakonec vyhodnotí.