Používání FireWire a USB portů a bezpečnostní aspekty pamětí typu „flash“

Metodický pokyn, verze 1

Praha, duben 2007

Obsah:

Používání FireWire a USB portů
a bezpečnostní aspekty pamětí typu „flash“

Metodický pokyn, verze 1, duben 2007

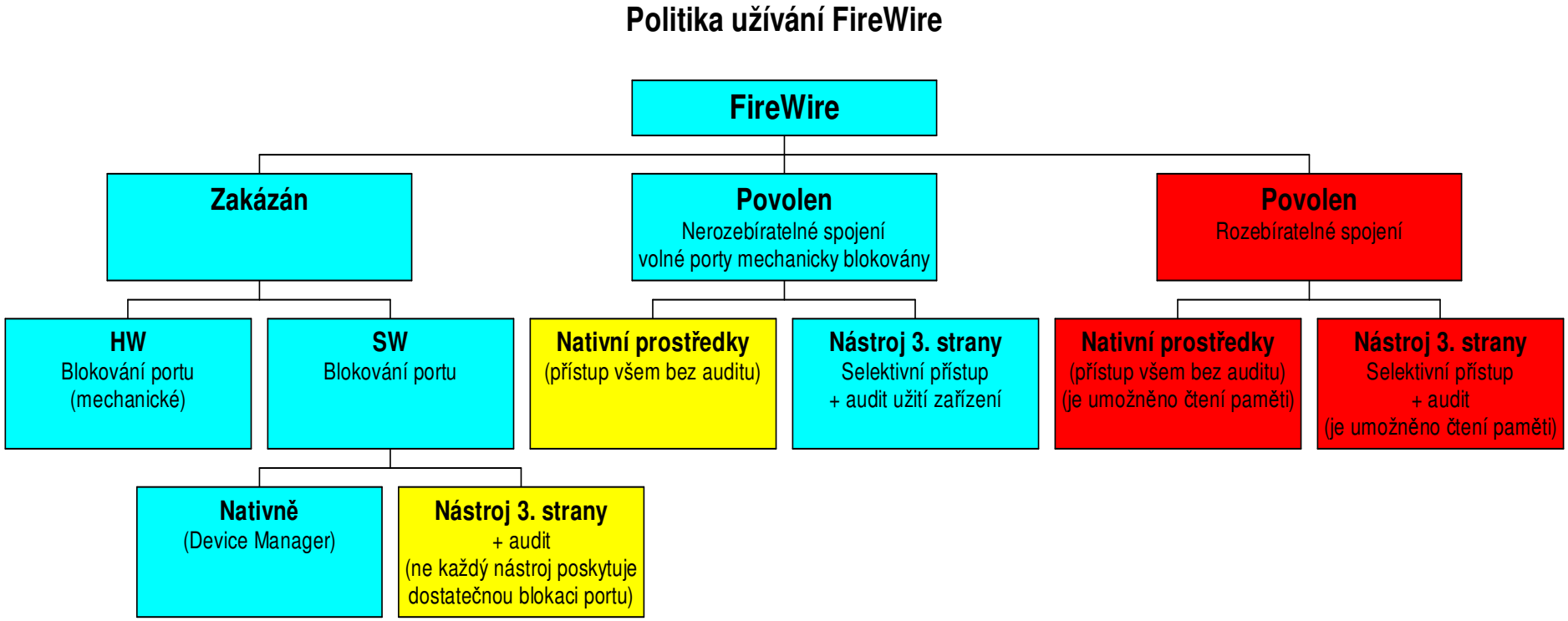
1. Úvod

Při certifikaci informačních systémů, v souladu se zákonem č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti a vyhlášky NBÚ č. 523/2005 Sb. o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, se stále častěji setkáváme s požadavkem použití FireWire a USB portů. Tento požadavek je do značné míry ovlivněn tím, že tato rozhraní jsou v současné době technologicky preferována a některá zařízení již neumožňují jiné připojení. Jako příklad mohou sloužit novější čtečky čipových karet nebo některé typy tiskáren a jiných periferních zařízení. Samostatnou otázkou je použití USB Flash pamětí (třída Mass Storage Device), které přinášejí uživateli značný komfort oproti jiným vyměnitelným médiím, ale jsou s nimi spojená také specifická rizika. Je třeba podotknout, že v některých instalacích, např. mobilní systémy, kde jsou limitujícími faktory prostor a vysoká míra spolehlivosti, je požadavek na jejich použití oprávněný nejen z hlediska poskytovaného komfortu.

V souvislosti s těmito požadavky oslovil NBÚ Elektrotechnickou fakultu ČVÚT a Vysokou školou chemicko-technologickou v Praze s požadavkem na řešení projektu „Zabezpečení USB portu a FireWire v operačních systémech Windows 2000 a Windows XP“ (číslo projektu ST20052006011) a „Bezpečnostní aspekty pamětí typu „flash““ (číslo projektu ST20052006010). Výstupem z těchto projektů byly závěrečné zprávy, které jsou uloženy na NBÚ. Na základě těchto závěrečných zpráv a s ohledem na vlastní zkušenosti a výsledky interního výzkumu zpracoval NBÚ následující metodický pokyn.

2. Politika pro bezpečné použití FireWire

Na základě provedeného výzkumu byly navrženy následující politiky pro bezpečné užívání FireWire a USB portů. Následuje grafické vyjádření pohledu na bezpečné používání FireWire. Pole vybarvená modrou barvou zobrazují stav s nízkou mírou rizika, kterou lze eliminovat standardními organizačními bezpečnostními opatřeními. Žlutá barva je použita u stavů, které vykazují střední míru rizika, ta může být částečně eliminována nadstandardními organizačními bezpečnostními opařeními a každý takový stav je nutné individuálně posuzovat. Červená barva je použita u stavů s vysokou mírou rizika, takové stavy nejsou v žádném případě doporučeny u systémů zpracovávajících utajované informace v souladu se zákonem č. 412/2005 Sb.



Z grafu je vidět, že pro prostředí, kde se vyžaduje vysoká míra bezpečnosti není možné povolit FireWire port ani za předpokladu, že se použije nástroj třetích stran. Důvodem je možnost přístupu do paměti počítače ze vzdálených uzlů.

2.1. Závěr pro bezpečné použití FireWire

Rozhraní IEEE1394 (FireWire) a jeho implementace ve formě OHCI kompatibilního řadiče zpřístupňuje vzdáleným uzlům (připojeným zařízením) celou fyzickou paměť počítače, a to pro obě operace čtení i zápis. Proto lze doporučit pouze mechanické blokování FireWire portu při současném zakázání portu prostřednictvím Device Manageru.

Pouze v odůvodněných případech mohou být k rozhraní připojena zařízení, která projdou schvalovacím procesem v rámci bezpečnostní politiky a budou splněny následující organizační bezpečnostní požadavky:

- bude mechanicky zajištěno, že žádné jiné zařízení se na daný port nepřipojí (mechanické zajištění kabelu + plomba). Schvalovací proces povolí pouze ta zařízení, u kterých se přesvědčí, že jejich firmware neobsahuje žádný kód, který by četl nebo modifikoval jiné části paměti hostitelského počítače, než ty, které potřebuje k vlastní činnosti,

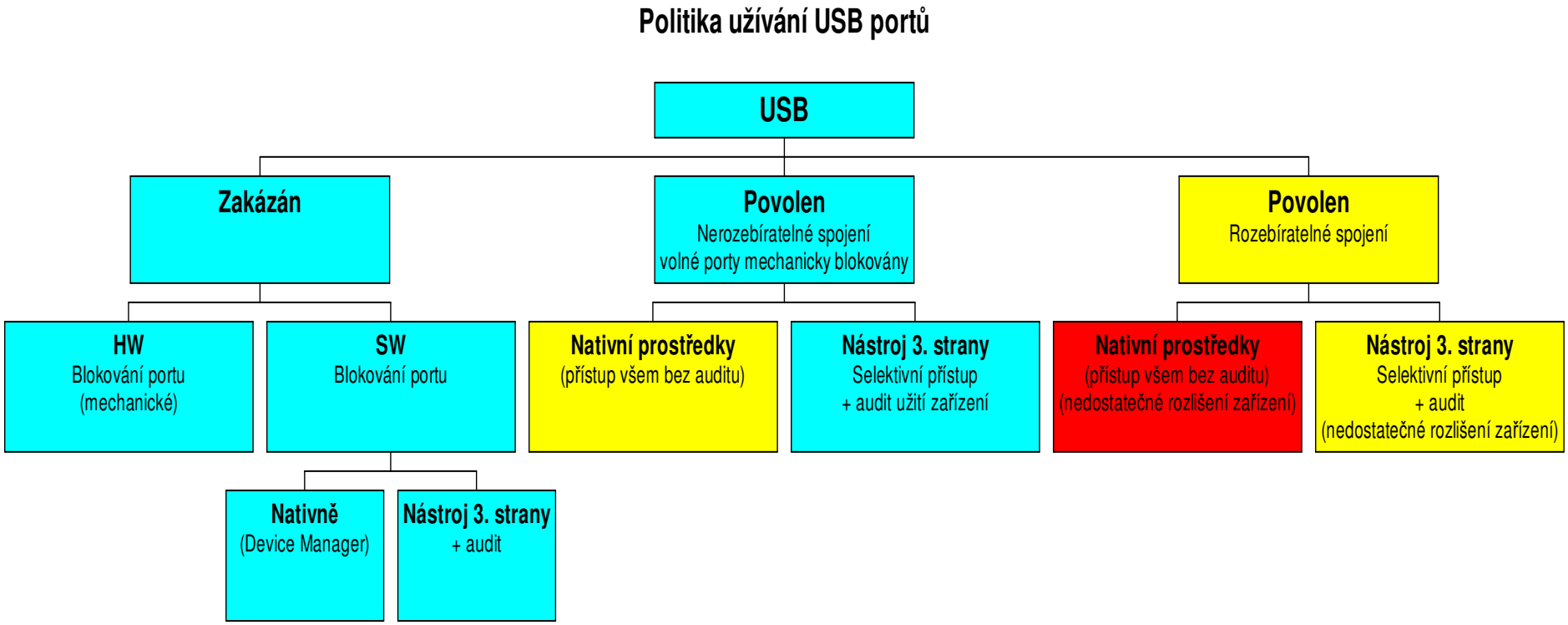
- bude instalován některý z doporučených nástrojů 3. strany umožňující vytvoření selektivního přístupu a bude zajištěno provádění auditu užití zařízení.

- celý informační systém bude instalován na režimovém pracovišti, nejlépe v zabezpečené oblasti odpovídajícího stupně, minimálně třídy II,

- bude prováděna pravidelná kontrola neporušenosti konfigurace informačního systému bezpečnostním správcem nebo jím pověřenou osobou a tutéž kontrolu bude provádět uživatel vždy před zahájením práce na informačním systému.

3. Politika pro bezpečné použití USB portů

Dále je uvedeno grafické vyjádření pohledu na bezpečné používání USB portů. Pole vybarvená modrou barvou zobrazují stav s nízkou mírou rizika, kterou lze eliminovat standardními organizačními bezpečnostními opatřeními. Žlutá barva je použita u stavů, které vykazují střední míru rizika, ta může být částečně eliminována nadstandardními organizačními bezpečnostními opařeními a každý takový stav je nutné individuálně posuzovat. Červená barva je použita u stavů s vysokou mírou rizika, takové stavy nejsou v žádném případě doporučeny u systémů zpracovávajících utajované informace v souladu se zákonem č. 412/2005 Sb.



Z grafu je patrné, že i v případě jasně mechanicky vymezené množiny připojených a prověřených zařízení, neposkytují nativní nástroje dostatečnou kontrolu nad přístupem uživatelů k zařízením.

3.1. Závěr pro bezpečné použití USB portů

U informačních systémů, které nevyužívají USB porty je požadováno provedení zákazu užití těchto portů a to buď mechanickým zablokováním nebo prostřednictvím nativních prostředků systému Windows XP nebo Windows 2003. Certifikace operačních systémů Windows XP a 2003 podle ISO/IEC 15408 (Common Criteria) z roku 2005 v sobě již zahrnuje hodnocení USB portů. V ostatních případech je nutné použít některý z doporučených nástrojů 3. stran.

V odůvodněných případech lze povolit realizaci nerozebíratelného spojení zařízení prostřednictvím USB portu při splnění následujících organizačních bezpečnostních opatření:

- bude mechanicky zajištěno, že žádné jiné zařízení se na daný port nepřipojí (mechanické zajištění kabelu + plomba). Schvalovací proces povolí pouze ta zařízení, u kterých se přesvědčí, že jejich firmware neobsahuje žádný kód, který by četl nebo modifikoval jiné části paměti hostitelského počítače, než ty, které potřebuje k vlastní činnosti,

- bude instalován některý z doporučených nástrojů 3. strany umožňující vytvoření selektivního přístupu a bude zajištěno provádění auditu užití zařízení,

- celý informační systém bude instalován na režimovém pracovišti, nejlépe v zabezpečené oblasti odpovídajícího stupně, minimálně třídy II,

- bude prováděna pravidelná kontrola neporušenosti konfigurace informačního systému bezpečnostním správcem nebo jím pověřenou osobou a tutéž kontrolu bude provádět uživatel vždy před zahájením práce na informačním systému.

V odůvodněných případech lze povolit realizaci rozebíratelného spojení zařízení prostřednictvím USB portu při splnění následujících organizačních bezpečnostních opatření:

- bude instalován některý z doporučených nástrojů 3. strany umožňující vytvoření selektivního přístupu a bude zajištěno provádění auditu užití zařízení,

- v rámci použitého nástroje bude zvolen princip **Whitelist**, kdy je primárně nastavena nejvyšší úroveň zabezpečení (vše vypnuto) a jen se přidávají do seznamu bezpečnostních opatření (whitelist) výjimky povolující vybraným uživatelům vybraný přístup,

- v rámci použitého nástroje bude povoleno pouze připojení takových zařízení, která umožňují jednoznačnou individuální identifikaci[1], tyto zařízení budou náležitým způsobem označena a evidována,

[1] Standardní popis zařízení obsahuje položku **Serial Number (SN).** Norma nevyžaduje, aby tato položka byla vyplněna. Pokud vyplněna je, tak musí být dle normy unikátní. Unikátnost je plně na zodpovědnosti výrobce. Pokud je přítomno SN, pak identitu tvoří trojice VID (**Vendor ID**), PID (**Product ID**), SN. Často se setkáváme s zařízeními, kde SN chybí např.u některých levných masově vyráběných USB zařízení.

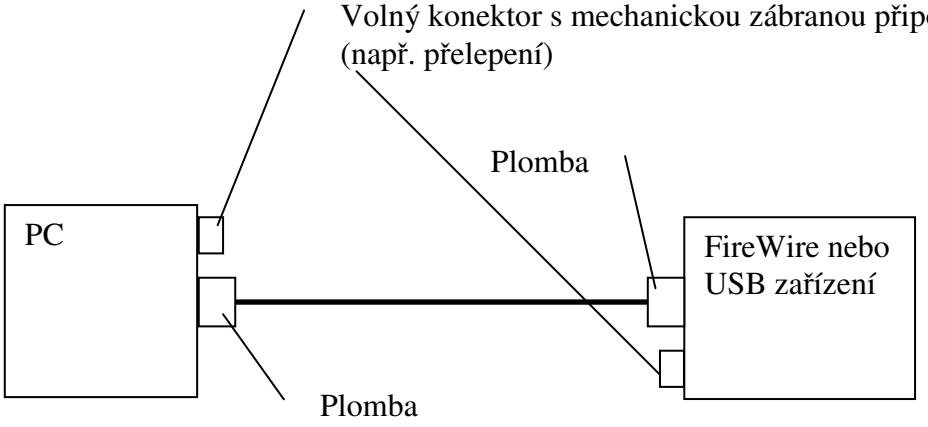
- celý informační systém bude instalován na režimovém pracovišti, nejlépe v zabezpečené oblasti odpovídajícího stupně, minimálně třídy II,

- bude prováděna pravidelná kontrola neporušenosti konfigurace informačního systému bezpečnostním správcem nebo jím pověřenou osobou a tutéž kontrolu bude provádět uživatel vždy před zahájením práce na informačním systému.

4. Doporučené postupy realizace bezpečnostních opatření

4.1. Zařízení připojená napevno pomocí nerozebíratelného spojení

Připustíme-li ztrátu schopnosti plug&play je možné propojit počítač s FireWire a USB zařízení pevným, neodpojitelným spojem. Např. standardní kabel FireWire mechanicky jištěný a plombovaný na obou stranách. FireWire a USB zařízení by pak mělo projít certifikačním procesem, že nezneužívá přímého přístupu do paměti.



Pevné připojení FireWire a USB zařízení

U volných konektorů musí být mechanicky zabráněno připojení zařízení, protože například FireWire se chová jako sběrnice, kde z každého uzlu jsou vidět všechny ostatní uzly.

V případě nerozebíratelného spojení zůstává na straně PC celý FireWire subsystém funkční a k selektivnímu přístupu k tomuto rozhraní (z pohledu uživatele) musíme použít některý z doporučených nástrojů 3. stran.

4.2. Zákaz použití celého portu na nejnižší úrovni

Zákaz použití celého portu můžeme provést následujícími způsoby:

- mechanické zabezpečení (odpojení portu, přelepení, zalití epoxidem, …),
- zabezpečení na úrovni BIOSu (zakázání používání portů a zařízení),

Tento způsob zabezpečení je použitelný bez ohledu na operační systém, ale umožňuje realizaci pouze zabezpečení typu použít/nepoužít, nelze při něm rozlišit různé uživatele, zařízení, typy přístupů a nelze tento způsob auditovat.

4.3. Zákaz použití paměťových USB zařízení nativními prostředky

a) Jestliže paměťové USB zařízení není v počítači dosud nainstalováno, odepřete uživateli nebo skupině oprávnění u následujících souborů:

%SystemRoot%\Inf\Usbstor.pnf,
%SystemRoot%\Inf\Usbstor.inf.

Provedete-li tuto operaci, nebudou uživatelé moci paměťové zařízení USB v počítači instalovat. Chcete-li uživateli nebo skupině odepřít oprávnění u souborů Usbstor.pnf a Usbstor.inf, postupujte takto:

1. Spusťte Průzkumníka Windows a vyhledejte složku %SystemRoot%\Inf.
2. Klepněte pravým tlačítkem myši na soubor **Usbstor.pnf** a poté klepněte na příkaz **Vlastnosti.**
3. Klepněte na kartu **Zabezpečení**.
4. V seznamu **Název skupiny nebo jméno uživatele** klepněte na uživatele nebo skupinu, kterým chcete oprávnění odepřít.
5. V seznamu **Oprávnění pro Jméno uživatele nebo název_skupiny** klepnutím zaškrtněte políčko **Odepřít** vedle položky **Úplné řízení** a poté klepněte na tlačítko **OK**. **Poznámka:** Kromě toho do seznamu **Odepřít** přidejte systémový účet.
6. Klepněte pravým tlačítkem myši na soubor **Usbstor.inf** a poté klepněte na příkaz **Vlastnosti.**
7. Klepněte na kartu **Zabezpečení**.
8. V seznamu **Název skupiny nebo jméno uživatele** klepněte na uživatele nebo skupinu, kterým chcete oprávnění odepřít.
9. V seznamu **Oprávnění pro Jméno uživatele nebo název_skupiny** klepnutím zaškrtněte políčko **Odepřít** vedle položky **Úplné řízení** a poté klepněte na tlačítko **OK**.

b) Jestliže je již paměťové zařízení USB v počítači nainstalováno, nastavte položku Start v následujícím klíči registru na hodnotu 4:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UsbStor

Provedete-li tuto operaci, nebude paměťové zařízení USB fungovat poté, co je uživatel připojí k počítači. Chcete-li nastavit hodnotu **Start**, postupujte takto:
1. Klepněte na tlačítko **Start** a potom na příkaz **Spustit**.
2. Do pole **Otevřít** zadejte příkaz **regedit** a potom klepněte na tlačítko **OK**.
3. Vyhledejte následující klíč registru a klepněte na něj:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UsbStor

4. V pravém podokně poklepejte na položku **Start**.
5. Do pole **Údaj hodnoty** zadejte hodnotu 4, klepněte na přepínač **Šestnáctková** (pokud již není vybrán) a potom klepněte na tlačítko **OK**.
6. Ukončete Editor registru.

4.4. Zákaz funkce Autorun

Automatické spouštění programu při vložení média je využíváno nejčastěji ke startu instalačních programů a interpretů multimediálních dat. Z tohoto důvodu je tento rys mezi uživateli oblíben. V operačních systémech Windows jej lze zakázat, a pokud není zakázán, funguje pouze pro vestavěné mechaniky (CD, DVD). Nicméně, vhodně naprogramované USB zařízení se může pomocí předstíraného Vendor ID prohlásit za pevnou mechaniku. V takovém případě, a pokud je autorun vůbec povolen, OS spustí program podle autorun.inf. V současnosti nejsou útoky vedené touto technikou považovány za vážné riziko. Platí princip, že všechny funkce a služby, které nemusí být spuštěné se u bezpečných systémů vypínají.

Autorun patří mezi rizikové faktory a v bezpečném systému by neměla být tato funkcionalita aktivní.

Způsoby povolení/zákazu funkce Autorun.

Nejčastější význam slova Autorun se váže na CD mechaniku. Ovládání této služby se nastavuje v registrech

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CDRom

Parametr **Autorun** má přednastavenou hodnotu 1, při její změně na 0 se při vložení CD „nespouští“.

S nastavením Autorun souvisí další dva klíče v registrech

1. NoDriveAutoRun

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\ Explorer

Hodnota parametru **NoDriveAutoRun** je určující pro blokování určitých písmen jednotek. Číslování je po jednotlivých bitech, jednotce **A:** přísluší první bit, jednotce **B:** druhý bit atd. Proto je hodnota parametru 0x00000005 pro jednotky A: a C:
Hodnoty parametru se pohybují v rozsahu 0x0–0x3FFFFFF
Přednastavená hodnota (default) je 0x0, čili všechny jednotky jsou povolené.

2. NoDriveTypeAutoRun

HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

Hodnota **NoDriveTypeAutoRun** určuje třídu zařízení. Pro hodnoty parametru v prvním bytu se stanoví, která zařízení mohou využívat službu Autorun. Pro provedení zákazu služby doporučujeme nastavení hodnoty na **0xFF**.

Tabulka uvádí nastavení parametrů pro jednotlivé třídy

Bit Number	Bitmask Constant	Description
0x04	DRIVE_REMOVEABLE	Disk can be removed from drive (such as a floppy disk).
0x08	DRIVE_FIXED	Disk cannot be removed from drive (a hard disk).
0x10	DRIVE_REMOTE	Network drive.
0x20	DRIVE_CDROM	CD-ROM drive.
0x40	DRIVE_RAMDISK	RAM disk.

V Resource Kitu pro Windows 2000 jsou uvedené hodnoty parametrů včetně neznámých typů a úplného blokování. Místo autorun je zde výraz autoplay.

Value	Meaning
0x1	Disables Autoplay on drives of unknown type.
0x4	Disables Autoplay on removable drives.
0x8	Disables Autoplay on fixed drives.
0x10	Disables Autoplay on network drives.
0x20	Disables Autoplay on CD-ROM drives.
0x40	Disables Autoplay on RAM disks.
0x80	Disables Autoplay on drives of unknown type.
0xFF	Disables Autoplay on all types of drives.

Autorun – spouštění programů při spuštění počítače

Dalším významem slova autorun je funkce spouštění programů při startu počítače. Opět jde o nastavení klíčů registrů, které určují posloupnost spouštění programů. Jedná se o důležitý bezpečnostní prvek, neboť zde je brána pro napadení počítače. Také zde je možné uložit programy, které zabezpečí skrytí skriptů při jejich běhu. Zobrazení procesu spouštění programů pomocí programu Autorun.exe poskytuje nativní nástroj MSCONFIG s možností nastavovat start jednotlivých služeb. Jedná se o důležitý nástroj pro řešení problémů.

Kritické je nastavení sedmi registrů, kde je uvedeno, které programy se spouštějí při startu počítače.

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ RunServices
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ RunServicesOnce
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ RunOnce\Setup

5. Nástroje 3. stran

Rozšíření operačního systému o nástroje třetích stran doplní chybějící funkčnosti a nastavení operačního systému především o:

- jemnější nastavení přístupových práv na úrovni uživatelů a zařízení,
- různé typy přístupů (čtení, zápis, bez přístupu),
- módy přístupu – permanentní, dočasný, plánovaný, online/offline,
- podpora většího množství typů zařízení – obsažena i podpora FireWire,
- definice a rozlišení různých typů zařízení i v rámci jedné kategorie a práce s nimi,
- rozšíření auditovacích schopností. (**Audit** je funkčnost, která sleduje aktivity uživatelů a ukládá informace o nejdůležitějších nebo vybraných činnostech do protokolu událostí. Zpětně lze tedy vysledovat činnosti jednotlivých uživatelů nebo aktuálně sledovat co kdo právě provádí.)

V této kategorii byly nalezeny následující nástroje:

Název	Výrobce / Dodavatel	Zdroj informací
Safend Protector	Safend Ltd., 32 Habarzel Street Tel Aviv 69710, Israel	www.safend.com
Device Lock	SmartLine Inc., 2010 Crow Canyon Place, Suite 100, San Ramon, CA 94583, USA	www.protect-me.com
Drive Lock	Headquarters, EMEA, Centennial Software Ltd, Wind River House 10 Viscount Way, Swindon, SN3 4TN, United Kingdom	www.centennial-software.com
DiskNetPro	DaVinsi - Content Security Solutions President Building Franklin Rooseveltplaats 12 b 25 B-2060 Antwerpen, Belgium	www.davinsi.com
Device Wall	Headquarters, EMEA, Centennial Software Ltd, Wind River House 10 Viscount Way, Swindon, SN3 4TN, United Kingdom	www.devicewall.com
Device Control	SecureWave Headquarters Atrium Business Park 23-ZA Bourmicht, L-8070 Bertrange Grand Duchy of Luxembourg Strom B-systems, s.r.o. Ohradní 1369/8 Praha 4 - Michle	www.securewave.cz www.securewave.com
SafeBoot	SafeBoot Corp. 2640 Golden Gate Parkway Suite 101 Naples, FL 34105 United States of America FreeDivision s.r.o. Poupětova 1339/3, 170 00 PRAHA 7 - Holešovice	www.safeboot.cz

5.1. Srovnání vybraných nástrojů třetích stran

Pro testování a zjištění možností zabezpečení USB a FireWire portů byly vybrány na základě dostupných informací a základních testů 3 produkty. Pří výběru byl kladen důraz na certifikace produktů, dostupnost materiálů o produktech a také reakce na dotazy ohledně testování produktů a možnosti jejich získání:

- Device Lock od společnosti SmartLine (www.protect-me.com)
- Sanctuary Device Control od společnosti SecureWave (www.securewave.cz)
- Safend Protector od společnosti Safend (www.safend.com)

Výběr byl proveden tak, aby byly pokryty všechny typy produktů od jednodušších až po komplexnější, popřípadě i dle získaných bezpečnostních certifikátů.

Vzhledem k neustálému vývoji produktů a rozšiřování jejich funkčnosti je platnost všech dále uvedených vlastností a výsledků testování časově platná k době, kdy byly testy provedeny.

Všechny produkty jsou plně kompatibilní s prostředím Windows 2000 a vyšším. Podpora pro Windows Vista, zatím není vzhledem ke stavu jejich uvolnění garantována a zaručena. Produkt Sanctuary Device Control podporuje také prostředí Citrix.

Z hlediska nasazení a srovnání produktů plyne:

- Device Lock – systém který je určený spíše pro menší sítě, protože náročnost na komunikaci je velmi vysoká, uživatelské rozhraní je komplikovanější a centrální správa je komplikovanější. Nástroj, který má sice delší historii, ale z pohledu trhu a rozšíření se jedná o nástroj nejnižší třídy, o čemž svědčí i neustálé rozšiřování, opravy produktu.
- Safend Protektor – produkt, který má dobré zabezpečující schopnosti, ale z pohledu podpory správy a dalších funkčností jako je centrální správa všech funkcí, včetně logování je zatím na začátku vývoje. Nevýhodou je také velká provázanost s infrastrukturou Windows (nutnost přístupu do GroupPolicy a její znalost). Je vhodný pro použití v prostředí, kde chceme mít možnost zablokovat bezpečně celý port např. pro případ omezení útoku přes FireWire port. Z pohledu trhu se jedná o produkt s kratší historií, o čemž svědčí především funkce, které v testované verzi poskytuje.
- Sanctuary Device Control – z pohledu poskytovaných funkcí se jedná o nejrobustnější nástroj, který je možné nasadit v libovolném prostředí. Jedinou nevýhodou je, že pracuje až na úrovni zařízení a tříd zařízení. Neumožňuje tedy zablokovat celý port USB a FireWire. Pokud se ale pracuje na úrovni zařízení Windows, tak splňuje všechny požadavky. Jedná se o nejstabilnější produkt i z pohledu trhu – získané certifikace, pozice na trhu, obsažené funkce.

Sanctuary Device Control - je stále v procesu hodnocení v souladu s ISO/IEC 15408 (Common Criteria) od roku 2003 s cílovou certifikací EAL 2.

Safend Protektor - je v procesu hodnocení v souladu s ISO/IEC 15408 (Common Criteria) od listopadu 2006 s cílovou certifikací EAL 2.

5.2. Nasazení produktů

Na základě veřejných informací a zkušeností lze doporučit nasazení produktů pro různá počítačová prostředí. Doporučení je shrnuto v následující tabulce.

Produkt	**Device Lock**	**Safend Protector**	**Sanctuary Device Control**
Samostatný počítač	ANO	NE	ANO
Málá síť (do 20 počítačů) Typ WORKGROUP	ANO	NE	ANO
Málá síť (do 20 počítačů) Typ ACTIVE DIRECTORY	ANO	ANO	ANO
Rozsáhlá síť	NE	ANO (pouze pro jednoduché struktury ACTIVE DIRECTORY)	ANO
Kombinovaná síť (počítači on-line i off-line)	NE	NE	ANO

Závěr

Na závěr lze konstatovat, že každý z těchto produktů poskytuje zabezpečení přístupu k zařízením připojeným přes USB, FireWire, případně jiných typů, ale před nasazením je třeba vždy zvážit všechny funkčnosti, které od zabezpečení očekáváme.

6. Použití USB Flash pamětí (třída Mass Storage Device)

6.1. Identifikace USB zařízení

USB identifikace je budována ve dvou nezávislých liniích. Budeme zde rozlišovat **taxonomickou**, **typovou** a **individuální** identifikaci.

Taxonomická identifikace

Taxonomická identifikace zařízení zařazuje do hierarchicky uspořádaných kategorií a je užitečná především při práci se zařízením, které nemá specifické ovladače, avšak je natolik jednoduché a běžné, že může být obsluhováno standardními ovladači. Stupně hierarchie taxonomické identifikace jsou tři:

- **Třída** – určuje druh zařízení. Příklad: třída Mass Storage zahrnuje všechny vnější paměti, tedy disky všech druhů, páskové paměti atd. Její číselný identifikátor je 8.
- **Podtřída –** určuje blíže druh zařízení v rámci třídy. Například, třída Mass Storage se dělí podle toho, jaké sady příkazů umí zařízení interpretovat. Jedna z podtříd je SCSI, tedy zařízení, které interpretují příkazy podle standardu SCSI.
- **Protokol –** zpravidla určuje, jak zařízení využívá prostředků protokolu USB.

Některé třídy mají zvláštní charakter

- **Prázdná třída** je použita v případě, že identifikace zařízení jako celku nemá význam a zařízení je považováno za soubor identifikovaných rozhraní.
- Třída **Human Interface Device (HID)** zahrnuje všechna zařízení, která tvoří rozhraní pro styk člověka se systémem. Nejčastějšími zástupci jsou myši a klávesnice; existuje však značné množství zařízení specializovaných. V praxi osobních počítačů jsou to v naprosté většině herní ovladače: volanty, knikly, pedály s mnoha vedlejšími prvky jako spouště, přepínače, atd. Z důvodů tak velké variability je definován jiný způsob popisu zařízení než v jiných třídách [2]. Podtřídy a protokolu se užívá jen u klávesnic a myší, které musí fungovat už při zavádění operačního systému. Úplný popis HID zařízení obsahuje pro každý ovládací prvek formát dat, které produkuje a jejich sémantiku.
- Třída **Vendor Specific** dovoluje definici libovolných podtříd výrobci zařízení. Jedinečnost identifikace podtříd není zaručena.

Typová identifikace

Konkrétní typ zařízení je určen **identifikátorem výrobce (Vendor ID, VID)** a **identifikátorem typu výrobce (Product ID, PID)**. Toto dvoustupňové schéma dovoluje každému výrobci s přiděleným VID používat PID podle vlastního uvážení. Obě složky identifikace mají jednak číselný, jednak textový tvar, aby programové vybavení nemuselo obsahovat převodní tabulky. Využití obou tvarů není standardizováno; ovladače operačních systémů Microsoft, které se vyhledávají podle číselného tvaru, obsahují samy lokalizovanou textovou podobu.

Individuální identifikace

Standardní popis zařízení obsahuje položku **Serial Number (SN).** Norma nevyžaduje, aby tato položka byla vyplněna. Pokud vyplněna je, tak musí být dle normy unikátní. Unikátnost je plně na zodpovědnosti výrobce. Pokud je přítomno SN, pak identitu tvoří trojice VID, PID, SN. Často se setkáváme s zařízeními, kde SN chybí. Tato volnost má ekonomické opodstatnění; u levných, masově vyráběných USB zařízení je velmi obtížné vytvořit technické prostředky pro realizaci individuálního výrobního čísla.

Závěr

U systémů zpracovávajících utajované informace v souladu se zákonem č. 412/2005 Sb. by měly být používány pouze zařízení umožňující jednoznačnou individuální identifikaci.

6.2. Životnost USB Flash pamětí a jejich vhodnost pro archivní účely

Základním nedostatkem Flash pamětí oproti jiným paměťovým médiím je omezený počet cyklů záznamu a mazání. Po jistém počtu cyklů vrstva GO degraduje - přestane plnit svojí izolační funkci a paměť přestane fungovat. Dnešní pokročilé výrobní technologie však umožňují vytvořit buňku která vydrží řádově až milion cyklů. V tomto směru jde vývoj poměrně rychle kupředu, stále se však můžeme setkat se staršími výrobky jejichž životnost se pohybuje kolem 10 tisíc zápisů. Na druhou stranu někteří výrobci koncových zařízení deklarují životnost až několik milionů zápisových cyklů. Toto je však nadsazený zavádějící údaj vycházející z předpokladu, že uživatel nebude nikdy přepisovat celou paměť a tudíž „chytrý“ kontrolér zajistí rovnoměrné rozložení zapisovací „zátěže“ mezi všechny buňky.

Základním materiálem pro výrobu Flash pamětí je monokrystalický křemík, pro vlastnosti výsledných struktur mají rozhodující vliv dielektrické vrstvy IPD a GO a materiál, ze kterého je vyrobena FG elektroda. Kvalita těchto materiálů určuje životnost pamětí z hlediska počtu zápisových a mazacích operací (degradace paměti, počet programovacích a mazacích cyklů) a doby udržení informace.

Mezi základní požadavky spolehlivosti Flash pamětí patří obvykle:

- garance bezchybného provozu paměťových buněk po minimálně 10^4 až 10^6 programovacích/mazacích cyklech,
- doba zapamatování informace minimálně 10 let.

6.3. Metody vymazání informací (bez destrukce média)

Bezpečným vymazáním se rozumí postup, kterým se znemožní (nebo se učiní vysoce obtížným) opětovné získání informací nejen v prostředcích IT ale i za použití speciálních laboratorních metod a prostředků.

Pro systémy s menší mírou rizika stačí trojnásobný přepis, například podle amerického standardu DoD 5220.22-M(E)[U17,U18] (první přepis pevně nastavenou hodnotou, druhý přepis náhodnou hodnotou, třetí přepis komplementární hodnotou k prvnímu přepisu) – metoda DoD I (DoD = Department of Defense (Ministerstvo obrany USA)).

Pro systémy s vysokou mírou rizika je nutný sedminásobný přepis např. opět podle amerického standardu DoD 5220.22-M (ECE). Metoda je známá pod zkratkou DoD II. Jde o dvojnásobnou aplikaci metody DOD I s proložením přepisem náhodnou binární reprezentací.

Poznámka 1:

Je třeba konstatovat, že výše uvedenými postupy založenými na přepisu nelze ovlivnit obsah bloků vyřazených v důsledku defektů a následného automatického přemapování paměti. Ani výrobci ani specializované firmy sice nenabízejí přečtení vyřazených bloků, ale nelze ho vyloučit. Existence těchto bloků tedy zůstává rizikovým faktorem vymazání citlivých dat přepisem. Pravděpodobnost přečtení zbytkové informace z přemapovaných bloků výrazně sníží softwarové šifrování dat.

Poznámka 2:

Působením vnějších fyzikálních veličin v rozsahu - teplota do 320°C, elektrické pole ~ 30 kV/cm, ionizující γ záření – Co 60 ~ 6 rad, vysokofrekvenční elektrické pole plazmového generátoru ~ 12,5 W/cm^2 v pásmu 14MHz dochází dříve k poškození podpůrných elektronických obvodů než vymazání uložené informace (ve sledovaném intervalu fyzikálních veličin nenastal případ, kdy by paměťové médium bezchybně fungovalo a uložená informace zanikla). Je třeba ovšem podotknout, že byly použity pouze laboratorně dostupné intenzity uvedených fyzikálních veličin.

Závěr

Mazání slouží pouze pro opětovné použití v rámci certifikovaného IS, nelze provádět deklasifikaci.

6.4. Metody likvidace informací (s destrukcí média)

V zásadě bude výhodné využívat takové provedení pamětí, u kterých je snadné demontovat plastový obal a následně např. horkým vzduchem odpájet vlastní čip paměti. Tím se redukuje objem a vznik toxických produktů při likvidaci paměti. Následnou destrukci paměti lze provést čtyřmi způsoby.

- Chemická likvidace – pomocí směsi kyseliny dusičné a kyseliny fluorovodíkové (jedovatá lázeň i produkty),
- Tepelná likvidace (zahřátím nad 2000°C) – hořák, vysokoteplotní odporová nebo induktivní pec, aluminotermická reakce (vše s odsáváním zplodin hoření).
- Mechanická likvidace nejlépe demontovaných čipů paměti (velikost částic na úrovni jednotlivých buněk tj. µm zrn) – drcení mlýny, rozbroušení.
- Nákup medii obsahujících elektrickou autodestrukční technologii např. flash media firmy Adtron s technologii ErasureZap.

Každá z uvedených metod má řadu výhod a nevýhod. Pro porovnání byla vybrána čtyři nejdůležitější hodnotící hlediska: realizovatelnost, produktivita, škodlivost (pro okolní prostředí), spolehlivost likvidace. Nákup medií obsahujících autodestrukční technologii nebyl hodnocen vzhledem k nesouměřitelným parametrům (náklady, specielní aplikace, dostupnost přenosného flash disku). Kolektiv autorů provedl celkové zhodnocení a po diskusi sestavil následující tabulku kde každé hledisko je hodnoceno stupněm 1 až 5. Přitom jednička znamená nejlepší hodnocení. Hodnocení počítá přibližně se stejnou váhou jednotlivých hledisek.

Hodnotící tabulka:

Likvidace:	**Chemická**	**Tepelná**	**Mechanická**
Realizovatelnost	4	2	1
Produktivita	2	2	2
Škodlivost	5	4	1
Spolehlivost	1	1	1
Σ	**12**	**9**	**5**

Závěr

Z hodnotící tabulky vyplývá, že nejvýhodnější metoda použitelná pro likvidaci dat je mechanická likvidace paměťových čipů. V současné době však nejsou k dispozici certifikovaná zařízení pro mechanickou likvidaci a proto lze doporučit tepelnou likvidaci při teplotě nad 2 000°C.

7. Literatura

[1] Závěrečná zpráva projektu, Zabezpečení USB portu a FireWire v operačních systémech Windows 2000 a Windows XP, Číslo projektu: ST20052006011, ČVUT v Praze FEL, Řešitelé: Miroslav Skrbek, Miloš Puchta, Pavel Náplava, Jan Schmidt, Rudolf Marek, Jan Mach, čj.: 441/2006-NBÚ/

[2] Zpráva o realizaci projektu, Bezpečnostní aspekty pamětí typu „flash“, Číslo projektu: ST20052006010, VŠCHT v Praze, Řešitel: Doc. Ing. Vladimír Myslík, CSc., Spoluřešitelé: Doc. Ing. Petr Macháč, CSc., Ing. Josef Náhlík, CSc., Ing. Přemysl Fitl, čj.: 672/2006-NBÚ/

Další odkazy na použitou literaturu jsou uvedeny u jednotlivých zpráv z řešení projektů.