Vysoká škola ekonomická v Praze

Fakulta informatiky a statistiky

Katedra informačních technologií

Studijní program: Aplikovaná informatika

Obor: Informatika

TPM – Trusted Platform Module

BAKALÁŘSKÁ PRÁCE

Student : Filip Eichenmann

Vedoucí : Ing. Luboš Pavlíček

Oponent : RNDr. Radomír Palovský, CSc.

2012

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a že jsem uvedl všechny použité prameny a literaturu, ze které jsem čerpal.

V Praze dne 9. května 2012 . . . . . .

Filip Eichenmann

Abstrakt

Práce začíná popisem architektury čipu TPM a vysvětlením souvisejících pojmů. Dále jsou uvedeny základní funkce, které čip nabízí. V další části jsou představeny zásady pro implementaci a nasazení TPM, označované jako best practices a následně jsou obecně naznačeny možnosti využití čipu v praxi. Samostatná kapitola je zaměřená na kritiku TPM a vysvětlení jednotlivých argumentů. Větším celkem je představení programů, které TPM využívají a jejich porovnání v tabulce vzhledem k základním funkcím TPM. Programy byly rozděleny do tří skupin – přímá podpora v OS, předinstalované nástroje a samostatná komerční řešení. V poslední kapitole je představena konkrétní firma a její IT struktura. Na to navazuje navržení možných řešení, jak lze využít čip TPM v této dané situaci. Součástí je naznačení postupu při aplikování daných řešení. V závěru jsou shrnuty výsledky a přínosy práce.

Klíčová slova

TPM, modul důvěryhodné platformy, důvěryhodná platforma, Trusted Computing Group, integrovaný bezpečnostní čip

Abstract

The thesis begins with description of the TPM architecture and explanation of related terms. Basic functions of the chip are then described. The principles for implementation and deployment of TPM are introduced in the following part. These principles are reffered to as best practices. Then the possibilities of practical use of the chip are suggested. One chapter is specifically focused on the criticism of the chip and explains several arguments against its use. Software, which supports TPM, is discussed and compared in the next chapter. It is divided into three parts – direct OS support, preinstalled tools and commercial solutions. Last chapter focuses on one company and its IT structure. Several possible solutions based on TPM are introduced for this particular situation. Every solution is described in more detail with suggested steps for deployment. The conclusion summarizes the results of the work and its benefits.

Keywords

TPM, Trusted Platform Module, trusted platform, Trusted Computing Group, embedded security chip

Obsah

Úvod

Bezpečnostní prvky se nejen v oblasti informačních technologií vyvíjí rychlým tempem. Nové možnosti techniky většinou znamenají nové typy hrozeb a útoků. Existují ovšem technologie, které jsou zde již dlouhou dobu, ale zdaleka nejsou využívány na všech platformách, kde jsou dostupné. To může způsobit několik příčin, buďto se technologie neověřila jako úspěšná, odborníci se neshodli na účinnosti nebo je technologie zastaralá. Mezi takové technologie patří i čip Trusted Platform Module (dále TPM), který je instalován do počítačů od roku 2003, ovšem dodnes není považován za doporučený standard v oblasti bezpečnosti a mnoho firem ho nezahrnuje mezi používané IT bezpečnostní prvky ani, pokud je k dispozici na zakoupených koncových zařízeních. TPM se dodává nejčastěji v přenosných počítačích v tzv. business třídě a v nejvybavenějších řadách výrobců, ale je osazován i do dražších základních desek pro stolní počítače. Někteří výrobci ho dodávají v hotových sestavách, určených většinou pro firmy, např. stroje Lenovo ThinkCentre.

Cílem této bakalářské práce je popsat čip TPM, jeho funkce a možnosti využití, včetně best practices, uvést přehled aktuálně prodávaných produktů s TPM, popsat software, který je dodáván výrobci přenosných počítačů pro podporu čipu TPM a popsat využití TPM s programy pro šifrování pevných disků. Další částí bude vysvětlení tvrzení, která poukazují na nevýhody TPM, kritizují některé vlastnosti a principy práce čipu a ve výsledku ho nedoporučují využívat jako součást bezpečnostních prvků, či dokonce považují TPM jako celek za nebezpečný a zbytečný. V samostatné části bude analyzováno zabezpečení v konkrétní firmě, respektive jeho část týkající se šifrování, práce s TPM a programů k tomu využívaných. Následovat bude návrh, jak by se mohlo využít funkcí TPM, jak při zachování současně používaných programů, tak s použitím nového software.

O míře bezpečnosti a využitelnosti TPM není dodnes definitivně rozhodnuto. Žádný bezpečnostní prvek sice nemůže být 100% odolný proti všem útokům, ale TPM se ani přes „pozitivní“ odborné články a doporučení nestalo celosvětovým bezpečnostním standardem ve firmách. Na druhou stranu „negativních“ článků lze nalézt na internetu zhruba podobné množství. Studiemi, které se snaží upozornit na problémy specifikace TPM a na možné hrozby, které mohou kvůli nim teoreticky nastat, se budu zabývat ve zvláštní kapitole.

V rámci této práce budu vždy využívat operační systém Microsoft Windows (od verze XP až po aktuální „beta“ 8 Consumer Preview). Je to částečně z toho důvodu, že Linux se ve firemním prostředí na klientských PC téměř nevyskytuje, to platí i pro MacOS X, který se sice pomalu začíná prosazovat v některých firmách, ale pro tradiční společnosti má pořád množství nevýhod (zejména v bezpečnosti a SW kompatibilitě) a zavedený Windows zatím nemůže nahradit.

Zdroje

Zdroje k tématu této práce lze rozdělit do několika oblastí. Nejvíce informací lze získat přímo u tvůrce – na webových stránkách organizace Trusted Computing Group (dále TCG) [1]. V sekci pro vývojáře jsou k dispozici pohromadě všechny soubory týkající se TPM, od plné specifikace, přes stručnější přehled architektury až po sekci často kladené dotazy. Soubory a specifikace se upravují, vše je důsledně verzováno a je možné stáhnout si kromě nejaktuálnější verze i ty předchozí.

Na téma týkající se TPM nebo jeho využití bylo napsáno několik bakalářských a diplomových prací, které většinou popisovaly konkrétní případ použití. Dvě jsou zaměřené na SW emulaci funkcí TPM, třetí se týká možné spolupráce TPM a open source šifrovacího programu TrueCrypt. Poslední práce se zabývá využitím TPM na platformě Linux.

- Trusted Platform Module a jeho emulácia [2]
- Trusted Platform Module a jeho emulace [3]
- Využití modulu důvěryhodné platformy pro podporu systému TrueCrypt [4]
- Principy a využití modulu důvěryhodné platformy [5]

Databáze ACM Digital Library patří mezi plnotextové specializované zdroje, dostupné na naší škole. Nachází se zde desítky odborných článků a záznamů z vědeckých konferencí, mnoho z nich se týká TPM jen okrajově, např. jako vedlejší možnost posílení zabezpečení. Několik článků, respektive prací se však velmi podrobně zabývá ochrannými prvky a celkovými možnostmi čipu.

K popisu software jsem využíval nejčastěji dokumentaci přímo od výrobce, případně propagační materiály pro firmy, které obsahují přehled o funkčnosti programu a některé

důležité vlastnosti popisují detailněji. Nejpodrobnějším zdrojem jsou komplexní návody pro administrátory. Např. informace k programu Microsoft BitLocker Drive Encryption jsou přehledně dostupné v databázi Microsoft TechNet Library.

Ostatní zdroje jsou většinou články z internetových periodik nebo technických blogů typu představení nové technologie, porovnání s existujícími a případné doporučení jejího využití. V oblasti software potom články srovnávající jeden typ programu (např. šifrovací programy), s ohodnocením funkcí a vybráním nejlepšího řešení.

1 Trusted Platform Module (TPM)

TPM je elektronický čip, umístěný na základní desce počítače nebo notebooku (případně i v mobilních zařízeních, jako jsou tablety a mobilní telefony, kde se ale zatím nerozšířil). Samotný čip před ničím nechrání (ani když je aktivovaný), je třeba ho využít v kombinaci s patřičnými ovladači a programy. Po základním nastavení se dá použít buďto jako zabezpečené úložiště klíčů, certifikátů, a dalších nebo k aktivnímu ověřování aktuálního stavu platformy.

Čip je ovládán pomocí příkazů, které jsou definovány ve specifikaci TPM. Veškerou komunikaci s TPM zprostředkovává ovladač zařízení, tzn., posílá příkazy a přijímá jejich výsledek. Programy, které s TPM pracují, používají ke komunikaci tento ovladač.

Výrobci čipů se sice řídí specifikací, která ale není ve všech částech striktní, proto se jednotlivé čipy od různých výrobců liší. Je možné, aby existovaly čipy s odlišnou vnitřní strukturou a přitom vyhovovaly požadavkům specifikace. Tato skutečnost patří mezi často kritizované vlastnosti specifikace a bude dále popsána v kapitole přímo zaměřené na kritiku TPM.

Podle [6] bylo v roce 2008 vybaveno TPM čipy přes 150 milionů počítačů a notebooků. Předpovědi pro následující roky byly značně optimistické – silný nárůst na více než 250 milionů strojů v roce 2010. To by se znamenalo, že přes 90 % všech strojů obsahuje TPM. Aktuální údaje sice chybí, ale situace na trhu nenasvědčuje takovému rozšíření. Mezi běžnými „domácími“ uživateli je počet strojů s TPM zanedbatelný.

1.1 Trusted Computing Group (TCG)

TCG je neziskovou organizací vytvořenou za účelem zavedení a zlepšení standardů v oblasti bezpečnosti informačních technologií. Založena byla v první polovině roku 2003 a jedním z jejích hlavních a pravděpodobně nejznámějších produktů je vytvoření standardu a specifikace pro čip TPM. Termín Trusted Platform/Computing lze přeložit jako "důvěryhodná platforma". TPM čip je výsledkem mnoha postupných úprav specifikace, které probíhají od roku 2003 a v dnešní době je ve verzi 1.2. Od roku založení se působení skupiny rozrostlo a aktuálně se věnuje mnoha oblastem, včetně mobilních telefonů a technologií mobilní bezpečnosti. Vždy se jedná o rozšíření možností zabezpečení nebo

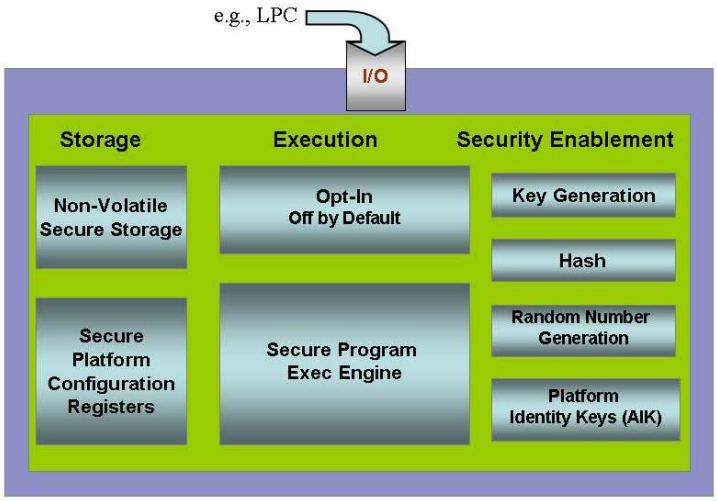
dosažení důvěryhodnosti při práci s daty na různých platformách vytvořením specifikace nebo standardu. Nicméně čip TPM je stále jádrem celého konceptu důvěryhodné platformy.

1.2 Části TPM

Podle [6] a oficiální specifikace TCG [7] lze strukturu čipu rozdělit na 3 části – funkční jednotky, non-volatilní paměť a volatilní paměť. Mezi funkční jednotky patří generátor náhodných čísel, SHA-1 hash generátor, HMAC generátor klíčů RSA, enkryptor/dekryptor RSA. V non-volatilní paměti jsou uloženy následující údaje a klíče:

- Endorsement Key (EK) – 2048 bitů
- Storage Root Key (SRK) – 2048 bitů
- Attestation Identity Keys (AIK) – 2048 bitů
- Owner Auth Secret (OAS) – 160 bitů

Ve volatilní paměti jsou sloty pro RSA klíče a PCR[1] hodnoty registrů. Jejich počet záleží na výrobci čipu. Dále jsou zde uloženy klíče a další potřebné parametry aktuální relace. Jako příklad poslouží obrázek č. 1, který znázorňuje komponenty čipu TPM (existuje několik možností jak graficky zobrazit a seskupit jednotlivé komponenty uvnitř čipu).



Obrázek č. 1: Komponenty TPM [8].

[1] Platform Configuration Register

1.3 TCG Software Stack (TSS)

Je souhrn komponent pro podporu aplikací, které budou TPM používat. Je to rozhraní pro komunikaci s čipem přes ovladač zařízení. Ovladač je pouhý prostředník, který zpracovává příkazy a jejich výsledky mezi TPM a TSS. Hlavními funkcemi TSS jsou:

- rozhraní pro aplikace využívající TPM funkcionalitu (TSS API)
- synchronizovaný přístup k TPM (poskytuje TCSD – TSS Core Services Daemon)
- aplikace se nemusí starat o problémy na nižších úrovních jako řazení a zarovnávání bajtů (poskytuje TSPI – TSS Service Provider Interface)
- správa prostředků TPM (poskytuje TCSD)

1.4 Funkce TPM

Specifikace TPM [7] definuje čtyři skupiny ochrany dat.

1.4.1 Svazování (Binding)

Tradiční operace spočívající v použití veřejného klíče při zašifrování zprávy. K dešifrování je potřeba soukromý klíč, který může být spravován čipem TPM jako nepřenosný, v tom případě lze dešifrovat zprávu pouze s konkrétním čipem TPM, který soukromý klíč vytvořil. Pokud je použit přenosný klíč, který lze přenášet mezi TPM čipy, neposkytuje kromě šifrování a bezpečného uložení po dobu přítomnosti v čipu žádnou další ochranu.

1.4.2 Podepisování (Signing)

Podepisování vytváří na základě zprávy klíč pro vygenerování podpisu. TPM označí některé spravované klíče jako „pouze pro podpis“, což znamená, že tyto klíče jsou použity pouze pro výpočet hash hodnoty podepsaných dat a zašifrování hashe. Proto nemohou být zneužity jako náhrada šifrovacích klíčů.

1.4.3 Zapečetění (Sealed-Binding = Sealing)

Zapečetění posouvá *Svazování* ještě o krok dále, kdy zapečetěné zprávy jsou vázány na množinu specifických vlastností platformy, zvolených odesílatelem. Platforma musí být v konkrétním stavu, aby bylo umožněno dešifrování. Zapečetění spojuje zašifrovanou zprávu, respektive symetrický klíč, kterým byla zpráva zašifrována, s množinou hodnot registrů PCR a nepřenosným asymetrickým klíčem. Zapečetěná zpráva je vytvořena vybráním několika PCR hodnot a asymetrickým zašifrováním těchto hodnot spolu se symetrickým klíčem. TPM s asymetrickým dešifrovacím klíčem může dešifrovat symetrický klíč pouze tehdy, pokud platforma splňuje odesilatelem definované hodnoty PCR.

Zapečetění je jednou z nejsilnějších stránek využití TPM. Dodává jistotu, že chráněné zprávy lze zobrazit, pouze pokud je platforma funkční a s předem známými specifickými vlastnostmi.

1.4.4 Zapečetěné podepisování (Sealed-Signing)

Podepisovací operace lze také spojit s PCR hodnotami registrů za účelem zvýšení důvěryhodnosti platformy, která zprávu podepisovala. Ověřující strana vyžaduje, aby byla v podpisu zahrnutá konkrétní množina PCR hodnot. Podepisující strana v průběhu procesu podepisování přidá zjištěné hodnoty PCR do zprávy a do rovnice výpočtu podpisu. Ověřující strana si následně může zjistit a porovnat PCR hodnoty obsažené v podepsané zprávě, což je ekvivalentní se zkoumáním konfigurace platformy v době výpočtu podpisu.

1.5 Profil ochrany (Protection Profile)

Součástí specifikačních dokumentů je i [9][8], který podrobně definuje bezpečnostní prvky TOE[2]. Hlavní specifikace TPM pro implementaci čipu nestačí, při použití v PC nebo NB je nutné zároveň dodržovat specifikaci PC klienta (TCG PC Client Specific TPM). Je to z důvodu volnějších pravidel v případě hlavní specifikace, které jsou ale pro použití konkrétně v počítačích přísnější (možnost implementace vs. povinnost).

[2] TOE – zahrnuje konkrétní modul TPM, což znamená HW, FW a/nebo SW, který implementuje funkce podle hlavní specifikace a zároveň specifikace rozhraní PC klienta.

Životní cyklus TPM se z pohledu profilu ochrany skládá ze 7 fází:

1. Vývoj TPM
2. Výroba TPM – vytvoření klíče EK, testování TPM
3. Výroba a doručení platformy
4. Nasazení platformy – převzetí vlastnictví TPM/platformy
5. Registrace identity platformy – aktivace identity, vygenerování klíčů AIK
6. Provoz platformy – operace podporované TPM, údržba
7. Ukončení provozu a recyklace platformy – bezpečné vymazání všech dat a klíčů

Kromě životního cyklu jsou v první kapitole vymezeny uživatelské role, které se týkají TOE. Celkem je definováno 6 uživatelských rolí:

1. Vlastník TPM – Kontroluje používání klíčů EK a SRK, vytváří a ovládá AIK. Může částečně delegovat svá práva na ostatní uživatele.
2. Delegovaná entita – Vlastník TPM nebo delegovaná entita s adekvátní pravomocí může delegovat svojí autorizaci na vybrané příkazy TPM na jinou entitu.
3. Vlastník entity – Uživatel, který vytváří a definuje token vlastníka entity AuthData (bezpečnostní atribut, který je nezbytný pro uložení entity do TPM)
4. Uživatel entity – Uživatel, který používá uloženou entitu.
5. Uživatel používající operatorAuth – Autorizační data operatorAuth povolují této roli dočasně vypnout TPM.
6. Svět – Tato role je přiřazena všem uživatelům, kteří nespadají do žádné z výše uvedených rolí.

Dokument dále v podrobné kapitole definuje bezpečnostní problémy ve třech podkapitolách – *Hrozby*, *Bezpečnostní politiky organizace* a *Předpoklady*. Jednotlivé položky jsou přehledně v tabulkách. Každá položka má číslo, název a popis, protože se na ně v celém dokumentu zpětně odkazuje. Na tuto kapitolu navazují podobně uspořádané bezpečnostní cíle. Kapitoly jsou vzájemně provázané, což lze vidět na následujícím příkladu:

Hrozba č. 5, *T.Hack_Physical* – neoprávněná osoba může způsobit odhalení nebo změnu části TOE fyzickou manipulací s TOE.

Této hrozbě odpovídá, resp. kontroluje jí cíl č. 22, *O.Tamper_Resistance* – TOE musí odolat fyzické manipulaci a útokům.

1.6 Aktuální stav PC/NB s TPM na trhu

Všichni přední výrobci nabízí aktuálně podporu TPM v některých řadách svých produktů. Nejaktivnější je v této oblasti společnost Hewlett Packard, která vybavuje TPM čipy i notebooky střední třídy. U ostatních často platí vzorec, že TPM najdeme pouze v „business" strojích, případně jen v nejvybavenějších (a nejdražších) modelech. Tabulka č. 1 přehledně shrnuje situaci u jednotlivých výrobců.

Výrobce	NB - řada/model	PC - řada/model
Acer	ne	Veriton L, M, S, X, Z
Apple	ne	ne
ASUS	B53S	ne
Dell	Precision M	Optiplex
Fujitsu	Celsius	Esprimo P
HP	Folio, ProBook, EliteBook	Compaq Pro, Elite
Lenovo	ThinkPad T, X	ThinkCentre M
MSI	ne	Hetis
Samsung	NP600B5BI	nevyrábí
Sony	VAIO S, Z	nevyrábí
Toshiba	Tecra, Portégé Z	ne

Tabulka č. 1: Aktuálně dostupné modely NB/PC s TPM.

TPM nalezneme i na vybraných základních deskách, např. od firmy ASUS. Podle článku [10] bude bezpečnostní čip obsahovat i připravovaný tablet HP Slate 8 s operačním systémem Microsoft Windows 8 Professional[3].

[3] Edice Professional bude zahrnovat nástroj BitLocker Drive Encryption podle [11].

1.7 Případy užití

Čip se dá implementovat do mnoha zařízení v odlišných prostředích. Obecně poskytuje konkrétní čip důvěryhodné spojení, které zaručuje, že druhá strana může důvěřovat danému stroji, respektive uživateli. Nabízí se tedy využití pro zabezpečení distribuce digitálního obsahu pomocí DRM[4]. Příklad: stažení filmu s ochranou DRM, jehož přehrávání je vázáno na jeden konkrétní čip TPM. Soubor lze přesunout, ale na jakékoliv jiné konfiguraci přehrát nepůjde. Microsoft tímto způsobem použil čip ve své herní konzoli Xbox 360.

Úložiště čipu je vhodné využít pro privátní klíč různých certifikátů, např. na šifrování pošty nebo pro přihlášení k bezdrátové síti, která vyžaduje uživatelský certifikát. Privátní klíč opouští čip, pouze pokud je označen jako exportovatelný a nikdy ne v přímo čitelné podobě.

Podle [12] vyžaduje U.S. Army od roku 2006 čip TPM instalovaný na každém zakoupeném PC. Společně s technologií Intel Trusted Execution Technology chrání (pomocí HW) proces bootování proti SW útokům.

1.7.1 Best practices

Dokument z webových stránek TCG [13] obsahuje základní, obecně aplikovatelné postupy, doporučení a principy užívání a nasazování TPM. Je napsaný tak, aby ho pochopili i uživatelé a administrátoři bez patřičných technologických znalostí. Tým TCG v něm definuje a specifikuje doporučení v rámci tzv. best practices, která by měla být korporacemi využívána pro zajištění nejlepší možné funkčnosti a bezpečnosti.

TCG si stanovilo čtyři podmínky pro zlepšování infrastruktury a bezpečnosti platforem:

1. zachování soukromí, zpětná kompatibilita a plná kontrola vlastníkem
2. jednoduchost použití
3. navržení technologie, aby byla schopna spolupracovat
4. zajištění přenositelnosti a přístupnosti uživatelských dat, i když budou zabezpečená a chráněná

[4] Správa digitálních práv (anglicky Digital Rights Management)

Následující definice šesti zásad[5] (anglicky „principle“) se vztahují na technologie, které TCG podporuje v rámci Trusted Computing (TC). Modul důvěryhodné platformy TPM je však nejdůležitější součástí – v podstatě jádrem TC. V textu se, kvůli obecnějšímu zaměření, objevuje termín „technologie TCG", který se ale dá vztáhnout především na TPM, jako základ bezpečnostního systému TC.

Bezpečnost (Security)

Primárním cílem TCG je silná podpora pro bezpečnostní politiky vlastníka platformy. Zásada bezpečnosti má připomenout vývojářům a návrhářům řešení, že mechanismy poskytují pouze základ pro dosažení zabezpečené platformy. Technologie TCG neodolá všem útokům a měla by být jedním bodem v komplexnější bezpečnostní strategii.

Soukromí (Privacy)

Zásada soukromí uvádí doporučení, která by měla být dodržována v rámci ochrany osobních informací. Uživatel platformy by např. měl být informován o tom, že jsou aktivovány TCG technologie a měl by mít možnost je deaktivovat. Mělo by být zajištěno, že komponenty TCG nejsou využívány nevhodným způsobem pro shromažďování osobních údajů. Soukromé informace o vlastníkovi platformy by měly být pouze pod jeho kontrolou a informace o uživateli pod kontrolou uživatele. Nevyužívaná uložená data by měla být po daném časovém období smazána. Proporcionalita jako součást základního bezpečnostního modelu TCG specifikace říká, že privátní klíče, jako nejdůležitější prvky ochrany platformy, by nikdy neměly být zveřejněny. Např. klíč EK v TPM se stává identifikovatelnou osobní informací, protože čip TPM je vázán na danou platformu. Specifikace tedy zakazuje obecně jakékoliv použití klíče EK, kromě základu pro generování klíčů, které nemohou zpětně vést k odhalení EK.

Spolupráce s ostatními systémy (Interoperability)

Zásada spolupráce se týká použití technologií TCG ve spolupráci s dalšími systémy a říká, že by s implementací neměly být vytvářeny žádné nové překážky. Např. služba by neměla

[5] TCG hovoří o zásadách, které doporučuje firmám a vývojářům dodržovat, aby výsledný produkt splňoval dané cíle. Popisuje, jak správně přistupovat k jednotlivým výzvám nebo problémům, které nutně souvisí s požadavky na TPM. Tato ucelená doporučení pak prezentuje jako tzv. best practices.

pro přístup vynucovat použití TCG technologie, pokud není požadována daná úroveň bezpečnosti. Zásady spolupráce v podstatě definují, jaké chování je očekáváno od komponent, které vyhovují určitému standardu a co znamená standard. Cílem je podporovat spolupráci s okolím.

Přenositelnost dat (Portability of data)

Při použití TPM v rámci TCG prostředí se některé z šifrovacích klíčů zapečeťují. Existují dva typy hardwarové ochrany: chráněné úložiště a zapečetěné úložiště. Chráněné úložiště znamená, že klíče jsou spravovány čipem TPM, kdežto zapečetěné úložiště vyžaduje k úspěšnému přístupu, aby bylo zařízení TPM v konkrétním stavu. Tato funkce má mnoho výhod a dodržuje zásady bezpečnosti a soukromí, ale nepodporuje přenositelnost dat chráněných tímto způsobem. Proto byly vytvořeny přenositelné klíče, které lze přenést do jiného prostředí. Opatření zahrnuje možnost obnovy dat chráněných pomocí TPM, pokud čip nebo jiná část systému přestane fungovat. Pro data, zabezpečená technologiemi TCG a vázaná na platformu, by měla být poskytnuta možnost exportovat je z TCG systému. V opačném případě uživatel, pracující s takovými daty, by měl být upozorněn, že v případě problémů není možnost je exportovat a dojde k jejich ztrátě. Klíče uložené v TPM by měly být navrhovány jako nepřenosné pouze, pokud je nepřenosnost přímým bezpečnostním požadavkem.

Ovladatelnost (Controllability)

Zásada říká, že každý uživatel by měl mít možnost kontroly nad používáním TCG technologií, které mu patří. Používání těchto technologií by nemělo být nucené. Každý uživatel by měl mít možnost kompletně vypnout TCG funkcionalitu způsobem, který neodporuje politikám nastavených vlastníkem. V určitých oblastech bude porušení této zásady nevyhnutelné výměnou za kvalitnější zabezpečení. Jedná se např. o oblast financí a bankovnictví, kde může být vyžadován daný stupeň zabezpečení pro přístup k některým službám.

Pokud má zařízení více vlastníků, je nutné rozdělit funkcionalitu TPM, tak aby každý z nich mohl ovládat pouze část, která je v jeho vlastnictví. Některé bezpečnostní funkce tedy budou vždy aktivovány a ostatní funkce TPM budou ovládány vlastníky a mohou být podle situace buď aktivované, nebo deaktivované.

Jednoduchost používání (Easy-of-use)

Stručná zásada, která říká, že i pro netechnického uživatele by měly být TCG technologie a jejich používání srozumitelné. TCG doporučuje využití expertů na uživatelské rozhraní už od počátku procesu navrhování systémů. Důležité dodržení zásady se týká především společností, které po uživateli vyžadují aktivované TCG technologie pro úspěšné použití služby.

1.8 Kritika TPM

Jedním z důvodů, proč se TPM tolik nerozšířilo, jsou nedostatky, na které není jednoznačná odpověď/řešení. Často bývají popsané v odborných článcích a slouží jako podklad kritiky celého konceptu TPM. Několik důležitých argumentů proti TPM bude v této kapitole popsáno podrobněji.

1.8.1 Komplexita TPM specifikace

Přílišná složitost TPM specifikace v kombinaci s určitou mírou volnosti v některých částech může způsobit různé typy problémů. Každý výrobce si může danou část vyložit trochu odlišně a výsledkem je rozdílnost v čipech od různých výrobců. V horším případě může výrobce zneužít části specifikace, kde je mu ponechána volnost a vytvořit čip, který sice vyhovuje specifikaci, ale byl kompromitován.

1.8.2 Označení splnění požadavků specifikace (TCG Compliance)

Běžný uživatel nebo vývojář si nemá jak ověřit, že čip v jeho přístroji splňuje standardy TCG. Není k dispozici obecný test, který by se dal použít na čipy různých výrobců a reálně by ověřoval konkrétní funkce a reakce čipu. Ve studii [14] byla vytvořena sada testů pro ověření čipů TPM proti verzi specifikace, kterou údajně splňují. Výsledky potvrzují domněnku z úvodu, která říká, že dva čipy vyhovující stejné verzi specifikace mohou na příkaz odpovědět diametrálně odlišně (vyskytly se i případy, kdy čip vrátil potvrzovací kód *TPM_SUCCESS*, když měl identifikovat chybu. Další testování odhalilo, že některé čipy používají chybové kódy, které vůbec nesouvisí s obdrženými příkazy, což sice může být podle specifikace přijatelné, ale také může posloužit jako základ útoku.

1.8.3 Správa referencí na klíče a relace

Specifikace vyžaduje dodržování určitých kvalitativních standardů pro náhodnost ukládaných referencí. Aplikace tak mohou mít odkaz na referenci, která odkazuje na jiný klíč nebo relaci, než je očekáváno. To může v závislosti na aplikaci vést k neočekávanému chování a k porušení bezpečnostních politik uživatele. Např. pokud jsou data zapečetěná jiným klíčem, než bylo zamýšleno, může k nim osoba s právy na odpečetění neúmyslně získat přístup.

1.8.4 Přenositelné klíče

Kritika je zaměřená na přenositelné klíče, které v podstatě narušují základní bezpečnostní princip TPM (klíče nikdy neopustí čip). Ve výsledku jde o paradox, protože je nutné zajistit se proti případné poruše čipu nebo základní desky zálohováním informací z TPM. Na druhou stranu i přenositelný klíč je v chráněném úložišti uvnitř TPM bezpečnější, než při uložení na pevném disku.

1.8.5 Ochrana proti útočníkovi s administrátorskými právy

Týká se případu, kdy má útočník k dispozici administrátorská práva a může napadnout systém, BIOS, či přímo nastavení čipu TPM, resp. nedostatku obrany v takové situaci.

Multiplatformní open-source šifrovací software TrueCrypt oficiálně nepodporuje TPM čipy a v oblasti „Často Kladené Dotazy“ na své stránce [15] k tomu má následující vyjádření:

TrueCrypt nebude používat TPM čipy, protože nenabízejí žádnou ochranu, pokud má útočník k dispozici administrátorská práva. V takovém případě může resetovat čip TPM, uložit si obraz paměti RAM obsahující klíče nebo obsah připojených jednotek TrueCrypt. Dále TPM označuje za zbytečnou technologii, dodávající svým názvem falešný pocit bezpečí.

1.8.6 Ztráta kontroly – „Korporace ovládne Váš počítač!“

Celý projekt Trusted Computing a zákon TCPA[6], který byl v USA v jednání vyvolal na svém počátku obrovský zájem. Okamžitě se utvořilo hnutí "Against TCPA!"[7], které se snažilo informovat co nejvíce uživatelů o následcích, které je čekají, pokud zákon bude schválen. Hlavní součástí TCPA byl právě TPM čip, který měl zajistit jedinečnou identifikaci každého PC. Odpůrci byl celý projekt často označován jako nástup „Velkého Bratra“ (naplnění románu G. Orwella 1984). Pokud by zákon prošel a uskutečnila se negativní očekávání z letáků hnutí, kompletně by se změnil IT trh, internet a v podstatě by vymizel svobodný SW a anonymita. Součástí byla vynucená aplikace technologie DRM, pro sledování a „ochranu“ veškerého obsahu na cílových počítačích. Představa, že někdo jiný bude rozhodovat o veškerém chování počítače a na majitele/uživatele nebude brát ohled, odradila uživatele od podobných technologií.

Tento bod byl pravděpodobně klíčovým argumentem proti rozšíření TPM. Organizace TCPA se přejmenovala na nynější TCG, ale TPM si cestu k uživatelům nenašlo ani „nenásilnou“ cestou. V době kauzy vzniklo i propagační video [16], které problém přiblížilo i lidem bez technického vzdělání.

1.8.7 Nedostatečné fyzické zabezpečení

Čip TPM verze 1.2 už se podle [17] podařilo fyzickou cestou prolomit. Navzdory opatřením proti takovému útoku se po šesti měsících snažení Christopher Tarnovsky dostal k uloženým klíčům na čipu s procesorem Infineon SLE 66CLX360PE. Jednalo se o čip v herní konzoli Microsoftu (Xbox 360). Firma Infineon od té doby nahradila tuto řadu novějším modelem, který má zabezpečení na vyšší úrovni.

Sama organizace TCG v dokumentaci tvrdí, že TPM nemůže odolat 100 % fyzickým útokům. Výrobci čipů mají relativní volnost v dodatečném HW zabezpečení, které je na velmi dobré úrovni. Až na tento incident nebyly další úspěšné útoky prokázány.

---

[6] Trusted Computing Platform Alliance

[7] Web http://www.againsttcpa.com/ už není aktivní, dohledat lze ve webovém archivu http://web.archive.org/web/20071130013415/http://www.againsttcpa.com/index.shtml.

1.9 Budoucí vývoj TPM

TPM čipy se budou nadále dodávat v business počítačích vybraných výrobců, ale o další verzi specifikace TPM informace zatím k dispozici nejsou. Microsoft a jeho nástroj BitLocker počítá s TPM i v připravované příští verzi Windows 8 a některé z možností TPM využijí i nové bezpečnostní funkce v procesu spouštění počítače. TPM pořád bude sloužit jako úložná jednotka pro certifikáty a klíče. S příchodem oficiální vědecké studie, která by dokázala, že existující TPM jsou bezpečné, by se jejich používání mohlo rozšířit, naopak v případě prokázání nedostatečného zabezpečení by byla technologie postupně méně a méně viditelná a používaná.

V oblasti šifrování nahradí postupně pevné disky s HW šifrováním (dále SED[8]) standardní SW řešení. TCG se momentálně zaměřuje právě na tuto část trhu [18]. Pro SED řešení připravila TCG specifikaci, podobně jako u TPM. Otevřené standardy jsou přístupné pro různé výrobce. SED přináší vyšší úroveň zabezpečení pomocí automatického šifrování, které je pořád zapnuté a funguje transparentně, není nutné instalovat další SW. Šifrovací klíče se generují přímo v disku a nikdy ho neopustí. Šifrování zajišťuje procesor, který je také součástí jednotky, což znamená téměř nulové omezení výkonu počítače. Autentifikace uživatele je prováděna diskem, nezávisle na operačním systému. Jednoduché je i bezpečné smazání disku – stačí resetovat disk (vygenerují se nové šifrovací klíče) a stará data již nebudou přístupná. Všechny tyto vlastnosti jsou ne nepodobné těm, které v této oblasti nabízí TPM, což by mohlo znamenat značné snížení jeho využití. Vzhledem k tomu, že šifrovací nástroje jsou hlavní oblastí, která využívá výhody čipu TPM, lze v případě rychlého rozšíření SED předpokládat postupné nahrazení nebo doplnění funkčnosti TPM.

[8] Self-encrypting drive – automaticky šifrovaná jednotka

2 Software

Většina výrobců notebooků instaluje na své stroje upravený OEM systém Windows s předinstalovanými aplikacemi pro využívání specifických funkcí daného počítače. V oblasti šifrování a bezpečnosti to platí dvojnásobně, proto bývá čip TPM prezentován jako důležitá funkce a instalovaný software se soustředí na šifrování, ukládání hesel a certifikátů nebo vytváření skrytých oddílů na disku, to vše s použitím TPM. V následující kapitole popíši tyto programy podle jednotlivých výrobců a porovnám s alternativou přímo od Microsoftu v podobě nástroje BitLocker Drive Encryption. Jednotlivé produkty se liší i ve využití možností bezpečnostního čipu TPM. IBM, Lenovo, HP i Microsoft podporují organizaci TCG a její cíle a patří mezi tzv. Promoters [19]. V oblasti freeware nebo open source nejsou programy implementující možnosti TPM tolik rozšířené, proto se v popisu zaměřím na komerční aplikace, určené především pro platformu Windows.

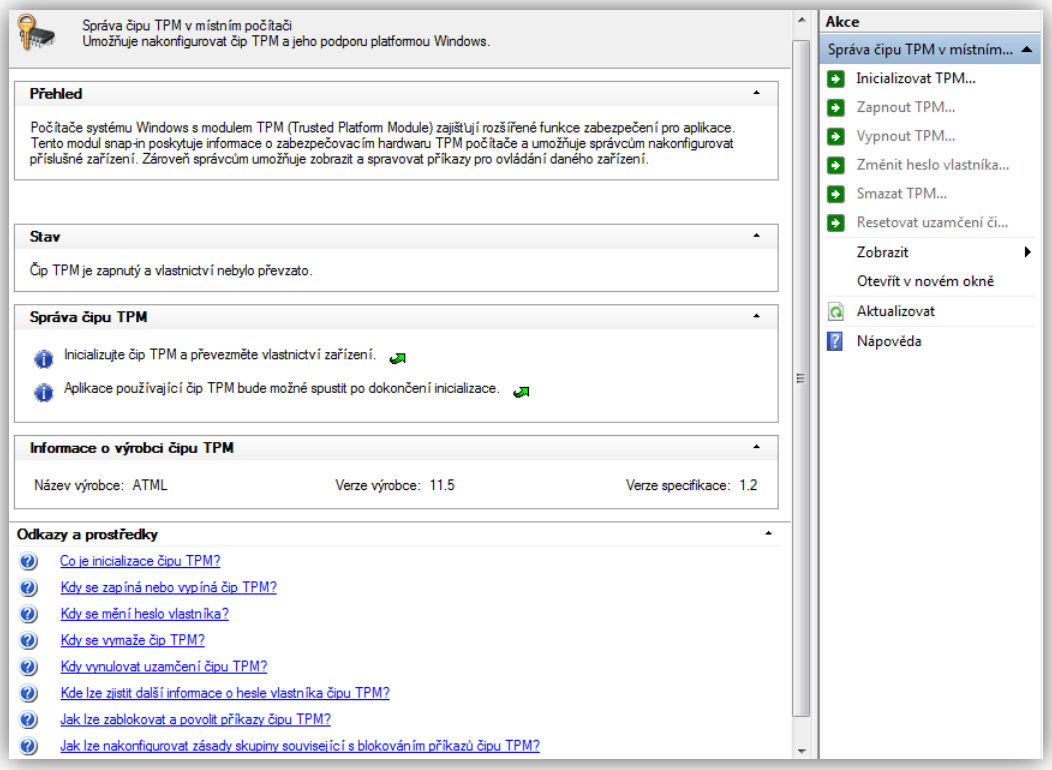
2.1 Podpora TPM v OS

2.1.1 Linux

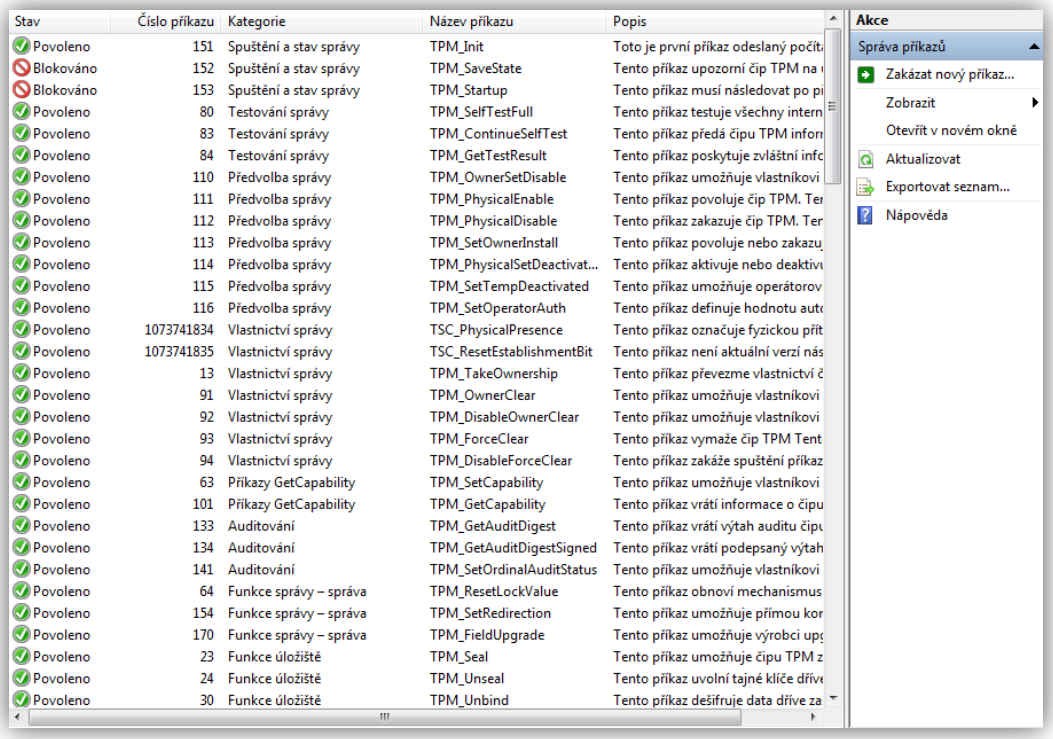
V jádře operačního systému Linux jsou zabudovány ovladače a podpora pro TPM čipy již od verze 2.6.12, vydané v červnu 2005.

2.1.2 Microsoft Windows

Podpora pro jednoduchou základní správu čipu je přímo integrovaná v OS ve formě modulu konzoly MMC. Na obrázku č. 2 je vidět hlavní okno s dostupnými funkcemi po pravé straně. Obrázek č. 3 ukazuje druhou dostupnou obrazovku se seznamem příkazů TPM a možností je blokovat.



Obrázek č. 2: Správa čipu TPM v Microsoft Windows.

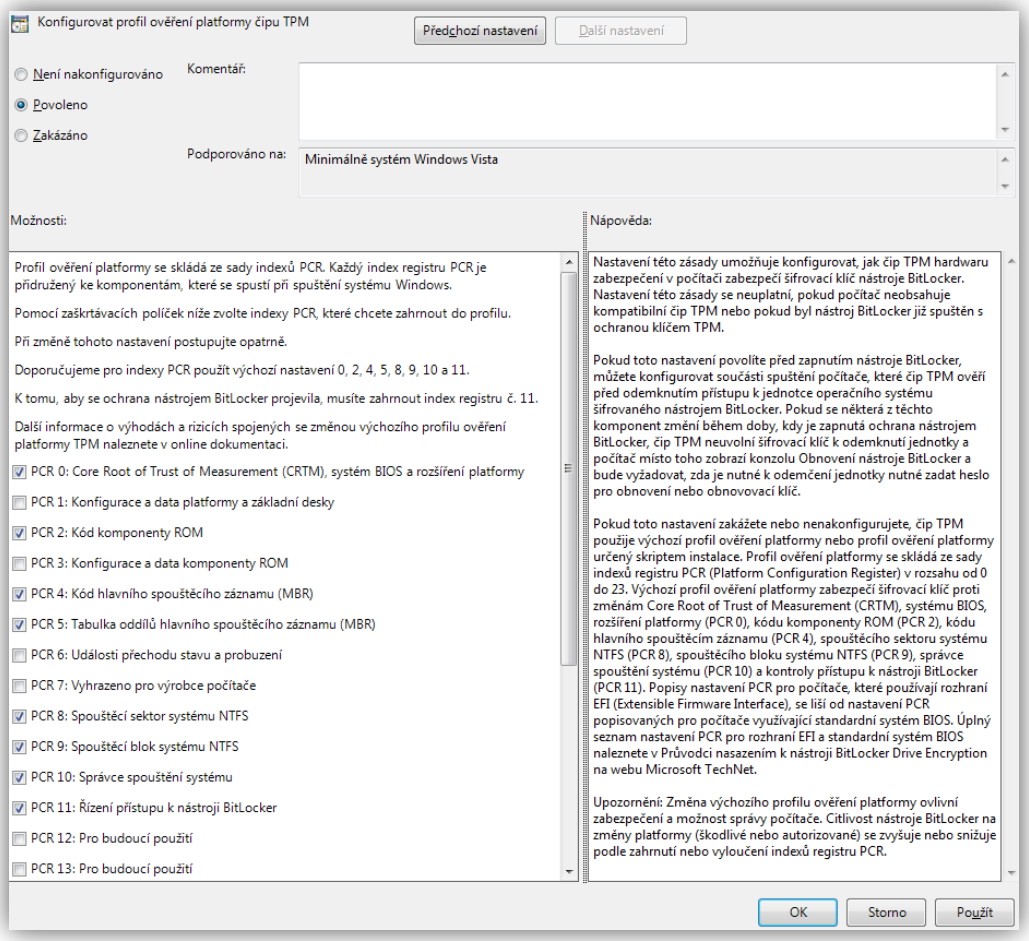


Obrázek č. 3: Správa příkazů čipu TPM v Microsoft Windows.

2.1.3 Microsoft BitLocker Drive Encryption

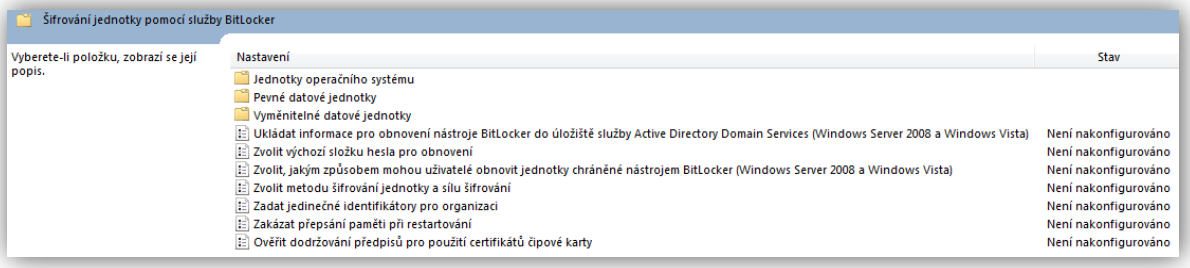
Microsoft nabízí vlastní řešení integrované v operačním systému Windows i v oblasti bezpečnosti. Poprvé se funkce BitLocker Drive Encryption objevila v roce 2006 v operačním systému Windows Vista. Jedná se o funkci, která je dostupná koncovým

zákazníkům nejen v nejvybavenější edici Ultimate, resp. Enterprise pro firmy s multilicenční smlouvou, ale i v serverové řadě Windows Server 2008. Bezpochyby nejrozšířenější verze Windows jsou Home Premium, následovaná edicí Professional, za což může kromě ceny také fakt, že minimum prodejců hotových PC sestav a notebooků zvolí jako předinstalovaný OS nejvyšší edici Ultimate. Ve firmách a školách nejrozšířenější verze 7 v edici Professional (ekvivalent edice Business v případě Windows Vista) sice podporuje práci s již zašifrovanými disky, ale neumožňuje je vytvářet ani spravovat nastavení šifrování. BitLocker umožňuje zašifrovat pevné disky, včetně systémových, ale nabízí i šifrování pro externí disky. Výkonnostně je rychlejší než software třetích stran (např. TrueCrypt), díky přímé integraci do Windows. Ve výsledku tak méně zatěžuje procesor a pevný disk. Klíčovou vlastností je pak podpora TPM čipů ve verzi 1.2. Uživatel má při přihlašování na výběr mezi použitím USB tokenu, TPM čipu, PIN hesla nebo různé kombinace těchto možností, viz [20]. Microsoft přímo doporučuje v rámci best practices používat kombinaci TPM a PIN heslo, viz [21] a [22]. Ve firemním prostředí se počítá s nasazením šifrování na koncové stanice, které budou pod správou IT oddělení a budou podléhat firemním politikám v doméně. Každý nový přenosný počítač musí mít aktivovaný a inicializovaný čip TPM, to znamená, že se vytvoří heslo vlastníka, které je uloženo v Active Directory Domain Services (AD DS). Ke každé šifrované jednotce je vytvořen obnovovací klíč, pomocí kterého ji lze dešifrovat (obnovovací klíče lze podle [23] také zálohovat do AD DS). Po připojení k jinému počítači se zašifrovaná jednotka chová jako běžný disk, zašifrovaný nástrojem BitLocker a k přístupu vyžaduje obnovovací klíč. Uživatel tedy pracuje s notebookem, chráněným čipem TPM, který ověřuje konfiguraci systému při každém spuštění (nastavení konkrétního ověřování viz obrázek č. 4), před načtením operačního systému musí zadat PIN heslo a následně ještě heslo do Windows při přihlašování v doméně.

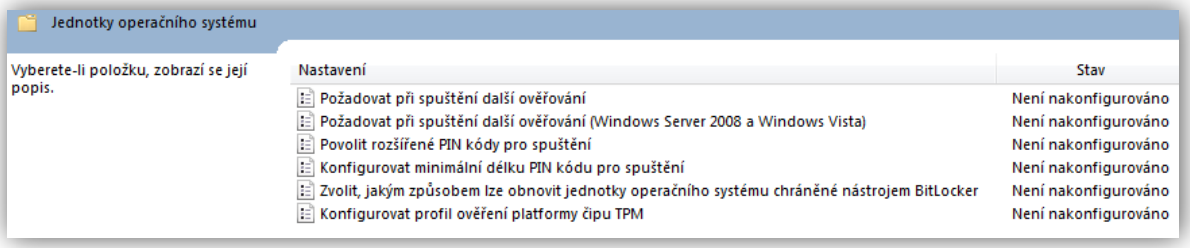


Obrázek č. 4: BitLocker – nastavení ověřování platformy pomocí PCR hodnot.

Nastavení nástroje BitLocker lze zahrnout do politik domény a vynucovat tak přesné vlastnosti šifrování, především způsob autentizace uživatele (povinnost např. TPM + PIN), sílu šifrování, minimální délku PIN, způsob obnovení zašifrované jednotky a další (viz obrázky č. 5 a 6).



Obrázek č. 5: BitLocker – Obecné nastavení parametrů šifrování.



Obrázek č. 6: BitLocker – Nastavení parametrů šifrování jednotky s operačním systémem.

V aktuálně vydané ukázkové verzi systému Windows je BitLocker integrován na první pohled bez změny od Windows 7. Přesto rozdíly existují a hned v průvodci spuštění nástroje je nová možnost automatické zálohy obnovovacího klíče do cloud úložiště Skydrive[9] (funguje, pokud je profil uživatele systému propojen s účtem Microsoft[10]). Přibylo možností nastavení (v Editoru místních zásad skupiny), ale grafické uživatelské rozhraní pořád chybí a některá nastavení lze provést pouze pomocí příkazové řádky[11]. V nových nastaveních lze povolit i funkci Secured Boot (viz následující kapitolu).

Nové funkce s podporou TPM ve Windows 8

Podle [25] a [26] přinese nová verze Windows tři nové funkce pro bezpečnější start systému. Jsou přítomné i v aktuální testovací verzi systému[12]:

- Secured Boot – Zabraňuje spuštění malware před startem systému pomocí ověření startujících komponent.
- Trusted Boot – Automaticky opravuje ovladače a vynucuje nastavení politik. Podporuje spuštění antimalware programů během spouštění, aby chránily PC ještě před dokončením procesu spouštění a přihlášení uživatele.
- Measured Boot – Spouštěcí procesy jsou podepsány, chráněny, změřeny a následně uloženy do čipu TPM, aby bylo zabráněno technologiím typu rootkit nebo malware. Každý start systému bude porovnávat hodnoty, aby byl proces ověřený.

[9] http://skydrive.live.com/

[10] Microsoft Account (= Windows Live ID) je účet používaný pro všechny online a mobilní služby společnosti Microsoft. S novou verzí Windows je více integrován do systému.

[11] Program manage-bde.exe je nástrojem na kompletní ovládání nástroje BitLocker, včetně konfigurace čipu TPM. Např. vynucení autentizace TPM + PIN lze nastavit pouze přes parametr tohoto programu. Seznam a nápovědu k příkazům popisuje [24].

[12] Microsoft Windows 8 Consumer Preview Verze 6.2 (Sestavení 8250)

2.2 Nástroje od výrobců notebooků a počítačů

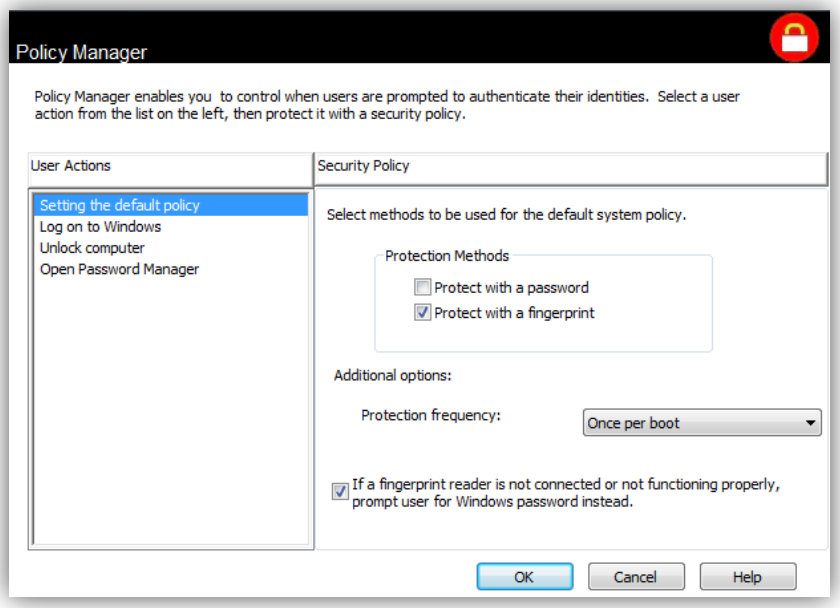
2.2.1 Lenovo ThinkVantage

Utility Lenovo jsou aktuálně sjednocené do sady technologií ThinkVantage. TPM se týkají tři – Client Security Solution, Password Manager a Fingerprint software. Speciální software pro šifrování pevného disku Lenovo nenabízí.

Client Security Solution (CSS)

Řešení bezpečnosti klienta – program, který uživatele informuje o HW bezpečnostních prvcích a nabízí jejich využití pomocí několika funkcí. Lenovo už program nenabízí skrz oficiální distribuční utilitu ThinkVantage System Update ani předinstalovaný na nových PC. Poslední verze byla takto dostupná pro Windows Vista. Nicméně vývoj programu je stále aktivní, nejnovější verze je ke stažení na webu[13]. Jednou z funkcí CSS je tzv. Audit, prověření všech hodnot bezpečnostních prvků a nastavení systému. Výsledkem je výpis a u každé položky porovnání s doporučenou hodnotou, a pokud je některá položka označena jako nebezpečná, je k dispozici odkaz na změnu/aktivaci správného nastavení. Největší předností programu je možnost importovat uživatelské certifikáty. Ty se ukládají do čipu TPM, což zaručuje vyšší stupeň ochrany (HW vs. pouze SW zabezpečení). Dále je možné řídit způsob přihlašování do Windows přes speciální nabídku *Policy Manager* (viz obrázek č. 7). Software pracuje s čipem TPM, čtečkou otisků prstů, nastavením hesel a programem Password Manager (instaluje se společně s CSS).

[13] http://support.lenovo.com/en_US/detail.page?LegacyDocID=MIGR-61432



Obrázek č. 7: Policy Manager – nastavení způsobu přihlašování uživatele.

Password Manager

Jednoduchý správce umožňuje ukládat hesla k webovým stránkám a při prohlížení je automaticky vyplňovat. Čip TPM je použit k zabezpečení hesel.

Fingerprint Software

Fingerprint Software obsahuje zároveň ovladač čtečky otisků prstů a zajišťuje její veškeré nastavení. Po instalaci je nastaven jako výchozí software pro manipulaci s otisky prstů, namísto vestavěné podpory ve Windows. Spolupracuje s CSS i s čipem TPM. Single Sign-On technologie dovolí uživateli přihlásit se pomocí jednoho ověření prstu i když je aktivováno Power-On nebo HDD heslo.

2.2.2 HP ProtectTools

Bezpečnostní řešení od HP, předinstalované na všech business noteboocích a vybraných business desktopech, je sadou programů pro aktivaci a nastavení jednotlivých technologií a bezpečnostních praktik, viz [27]. Pro podniky je k dispozici Central Management for HP ProtectTools, s možností spravovat software z jednoho místa. Enterprise verze umožňuje napojení na AD DS a instalaci i na počítače jiných výrobců.

HP ProtectTools zahrnuje

- HP Security Setup Wizard
- Enhanced Pre-Boot Security
- HP SpareKey
- HP ProtectTools Security Manager – Správce jednotlivých modulů, veškeré nastavení se provádí na jednom místě.
- Credential Manager for HP ProtectTools – Spravuje identitu uživatele a sdružuje všechny možnosti přihlášení (heslem, otiskem prstu, autentizací TPM, jiným tokenem). Pokud je k dispozici, chrání identitu uživatele čip TPM.
- Drive Encryption – HP spolupracuje s McAfee a předinstalovaný SW Drive Encryption je pouze jinak pojmenovaný McAfee Endpoint Encryption (dále EE), konkrétně jeho starší verze. Tato spolupráce trvá již několik let, kdy se produkt ještě nazýval SafeBoot Device Encryption a byl navržen a optimalizován speciálně pro počítače HP. Logo SafeBoot zde dokonce zůstalo a podle udávané verze se jedná o několik let staré sestavení (aktuální McAfee EE je v 6. verzi, zde je 4.).
- Privacy Manager – Přidává možnost odesílat podepsané a šifrované e-maily, dokumenty nebo zprávy. Pro bezpečnou komunikaci se používá Windows Live Messenger s přidanou funkčností. Konverzace je přenášena pomocí protokolu SSL/TLS místo protokolu XML. Dále lze ověřit příjemce, podepsat zprávu a šifrována je i historie konverzace.
- HP Disk/File Sanitizer – Bezpečně maže soubory nebo přepisuje prázdné místo na pevném disku.
- Computrace Pro for HP ProtectTools

Embedded Security for HP ProtectTools

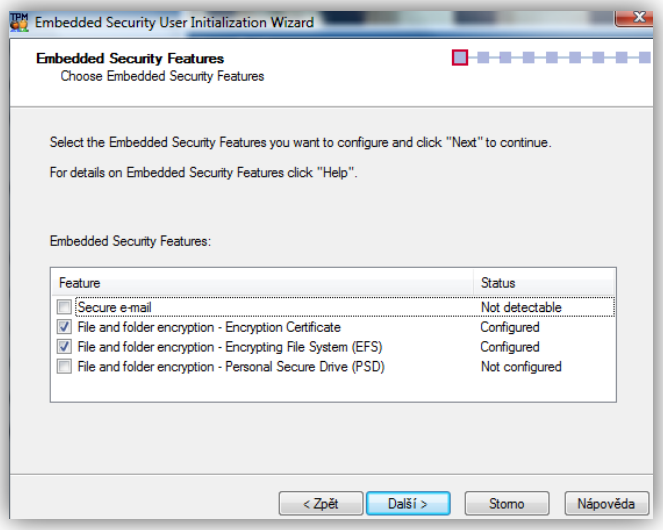
Plug-in pro Security Manager, který má pět hlavních funkcí (poslední čtyři jsou konfigurovatelné pomocí průvodce, viz obrázek č. 8):

- ovládání základních operací čipu TPM (povolení, inicializace, převzetí vlastnictví, resetování do základního stavu, zálohování, migraci a další)
- správa certifikátů v TPM (vytváření, import, export)

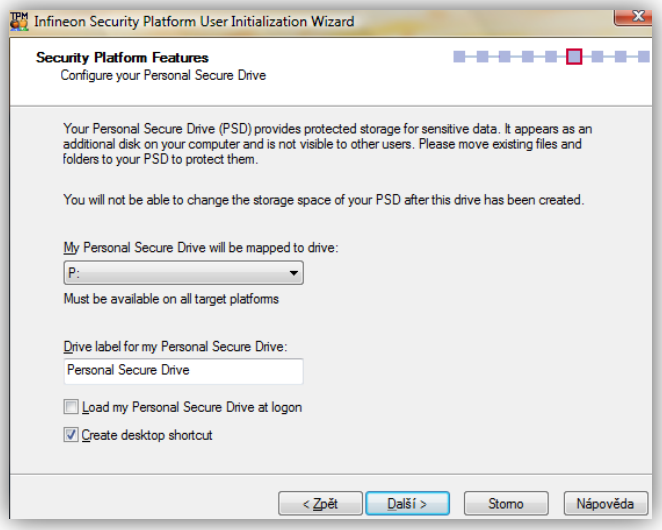
- šifrování jednotlivých souborů/složek pomocí systému souborů EFS[14]
- šifrování pošty
- vytvoření virtuálního šifrovaného disku (Personal Secure Drive, viz obrázek č. 9)

Před použitím šifrovacího programu se musí čip inicializovat přes tento SW (inicializaci lze jinak provést i pomocí správy čipu TPM od Microsoftu).

Jádro programu je totožné s oficiálním SW výrobce Infineon – Infineon TPM Professional Package, jedná se tedy pouze o integraci do řešení HP ProtectTools.



Obrázek č. 8: Funkce programu Embedded Security for HP ProtectTools.



Obrázek č. 9: Personal Secure Drive – nastavení osobní virtuální jednotky.

[14] Encrypting File System (EFS) – Šifrování jednotlivých souborů a složek na pevném disku pomocí certifikátu s privátním klíčem (ten je uložen automaticky do TPM v případě SW od HP/Infineonu). Podmínkou je OS Windows 2000 nebo vyšší a systém souborů NTFS.

2.3 Samostatná komerční řešení s podporou TPM

2.3.1 McAfee Endpoint Encryption

Společnost McAfee je podle Gartneru jedním z lídrů magického kvadrantu v oblasti ochrany koncových stanic. Už z nabízeného portfolia programů je zřejmé zaměření na business oblast a větší firmy. Domácí uživatel má kromě několika antivirových a antispamových řešení na výběr ještě zálohovací program, využívající cloud úložiště. SafeBoot byl dřívější název tohoto programu a zároveň firmy, která ho vyvinula.

Robustní řešení Endpoint Encryption obsahuje komponenty potřebné pro jednoduchý, centralizovaný provoz šifrování na mnoha cílových stanicích. Konkrétní řešení bývá pro každou firmu individuální, protože celý systém je vysoce modulární v možnostech kombinací serverů, databází a úložišť. Ověření uživatele je také možné pomocí řady standardů a jejich kombinací. Návod pro administrátory [28] podrobně popisuje výčet podporovaných způsobů přihlášení: Smart karty a USB tokeny, obecná podpora tokenů, certifikáty, Aladdin eToken 64KB, SafeNet IKEY 2032, EE Phantom USB biometrický klíč, UPEK čtečka otisků prstů, Infineon Embedded TPM čip a několik dalších. Požadavky na TPM čip jsou přímo specifikovány, musí jít o čip výrobce Infineon, vyhovující TCG specifikaci verze 1.2. Dále musí být nainstalován software Infineon TPM Professional Package[15], čip musí být inicializován, což zahrnuje vytvoření klíčů EK, SRK, nastavení vlastníka a jeho hesla. Je možné implementovat jen základní komponenty systému a později dokoupit další funkcionalitu, což šetří náklady. Základními komponentami jsou EE Manager, Server, Object Directory, PC Client, File Encryptor a Connector Manager.

EE Manager (dále EEM) je centrální částí systému a základem celé konfigurace. Administrátorské rozhraní je přístupné přes TCP/IP spojení pouze privilegovaným osobám.

EE Server (dále EES) zprostředkovává komunikaci s EEM, klientem a databází objektů přes IP připojení.

[15] Software pro kompletní správu nastavení TPM, není vázán pouze na čipy firmy Infineon.

EE Object Directory obsahuje všechny entity v systému EE, tzn. uživatele, stroje a nastavení. Tuto databázi lze provozovat na stejném serveru jako EES nebo samostatně (lze i duplikovat, zálohovat, vše záleží na specifickém prostředí a požadavcích dané firmy).

EE for PC Client – balíček, který musí být distribuován na všechny koncové stanice. Provádí synchronizaci s EEM, pokud se počítač připojí k nové síti nebo pokud je vyvolána ručně (vynucená synchronizace od administrátora nebo od uživatele). Po první instalaci se provede restart a otestuje se zavedení nového boot loaderu. Pokud vše pracuje správně, je instalace dokončena a lze synchronizovat nastavení s EEM. Umožňuje transparentní šifrování na pozadí, nevyžaduje k tomu zásah uživatele ani jeho přihlášení (pouze spuštěný počítač).

EE File Encryptor je modul nabízející možnost šifrovat jednotlivé soubory s pomocí různých klíčů/hesel. Lze vytvořit i záložní pár RSA klíčů pro dešifrování souboru při zapomenutém hesle.

EE Connector Manager umožňuje napojení EEM do používaných struktur třetích stran, především AD DS.

Jsou podporovány i vlastní algoritmy šifrování, ale doporučeným je AES-FIPS s 256bitovým klíčem. V systému EE Enterprise lze použít pouze jeden algoritmus, nikoliv kombinace.

2.3.2 Utimaco/Sophos

Společnost Utimaco (nyní Sophos) v minulosti spolupracovala s firmou IBM za účelem zlepšení šifrovacího procesu s využitím TPM bezpečnostních čipů na deskách ThinkPad a ThinkCentre strojů. Ještě v roce 2005, kdy počítačovou divizi IBM převzalo Lenovo, byla spolupráce s Utimaco aktivní, viz [29]. Aktuálně se již na nových PC a NB Lenovo software předinstalovaný nedodává a Sophos přestal podporu TPM uvádět ve specifikacích programů. Rozsah nabízených programů je široký, sahá od domácích uživatelů, až po enterprise řešení pro velké společnosti, viz [30]. Podle každoroční analýzy Gartner Magic Quadrant for Endpoint Protection Platforms patří Sophos mezi lídry na trhu pravidelně již od roku 2009.

Spolupráce Sophos a Lenovo je stále aktivní v oblasti integrace Sophos programů s Lenovo Rescue and Recovery, což je software na obnovu poškozených disků dodávaný na počítačích Lenovo.

SafeGuard PrivateDisk

PrivateDisk je, jako jediný program z původního komplexního řešení pro Lenovo, po registraci poskytován zdarma ke stažení[16], již bez dostupnosti podpory, aktualizací a pouze pro 32bitové operační systémy. Umožňuje vytvoření virtuálního soukromého oddílu na pevném disku, který je zašifrovaný a heslem chráněný. Potřebné klíče jsou uloženy v TPM a bez ověření uživatele není umožněn přístup k datům na jiném počítači (pouze pokud by byla administrátorem převedena na ekvivalentní ThinkPad). Program je dále vyvíjen a aktuální verzi lze zakoupit na webu Sophos.

SafeGuard LAN Crypt

LAN Crypt nabízí šifrování souborů sdílených v síti pracovní skupinou. Proces šifrování je automatický a běží transparentně na pozadí. Každý uživatel má svůj unikátní skupinový klíč a může přistupovat k souborům, zatímco neautorizovaná osoba uvidí jen nečitelná data. Existují dva typy „administrátorů“ – administrátor serveru a správce bezpečnosti. Tyto role jsou striktně odděleny, administrátor spravuje systém, ale nemůže dešifrovat žádné soubory a správce bezpečnosti spravuje jednotlivé uživatele, skupiny, práva a klíče. Pro uložení klíčů lze využít čip TPM.

SafeGuard Easy

Poskytuje šifrování kompletního disku na systémech Windows XP a novějších, včetně bootovacích disků. Lze instalovat v počítačové síti, bez nutnosti zásahu uživatelů. Podporuje jednotné přihlášení Single sign-on. Heslo se zadává před začátkem startování operačního systému. Verze Easy je navržena pro práci v prostředí, které není centrálně spravované. Pokud je centralizovaný management vyžadovaný, lze provést upgrade na verzi Enterprise, bez nutnosti dešifrovat a znovu šifrovat aktuálně používané stanice.

SafeGuard Enterprise

Enterprise verze kromě správy samotného programu nabízí podporu a centrální management pro pevné disky se zabudovaným hardware šifrováním (OPAL[17]) a pro nástroj BitLocker na stanicích s Windows Vista/7. Autentifikace uživatele je možná pomocí

[16] http://www.thinksophos.com/

[17] Opal Storage specifikace vytvořená TCG.

certifikátů, hesel, biometrických údajů, Single Sign-On, USB tokenů, použitím smart card nebo key ring. Pro obnovení poškozeného operačního systému ze zašifrovaného disku lze externě nabootovat do Windows PE.

2.3.3 Wave

Společnost Wave je jedním ze zakládajících členů konsorcia TCG. Propaguje využívání TPM čipů ve společnostech pomocí svých produktů, které se soustředí na centralizovaný management funkcí TPM. Dodává software předinstalovaný na počítačích Dell, Acer, NEC a dalších. Téměř všechny produkty z portfolia firmy [31] nějakým způsobem využívají TPM, proto bude řada EMBASSY popsána jako celek. Wave se zaměřuje také na pevné disky s HW šifrováním a jejich správu a v budoucnu předpokládá postupné nahrazení dnes stále běžnějšího SW šifrování.

Wave for BitLocker Management

Centrální správa pro nástroj BitLocker umožňuje aktivovat, monitorovat a ovládat jednotlivé klientské počítače. Navíc poskytuje automatický management TPM, šifrovaně zálohuje obnovovací klíče a kontroluje konfigurační parametry BitLocker.

Wave Encryption Service

Šifrování jako služba dostupná z cloudu, bez potřeby instalování programů třetích stran. Spravuje se přes webové rozhraní, podporuje BitLocker, Microsoft Encrypting File System (EFS), a SED. Počítače s podporou BitLocker jsou automaticky identifikovány a vzdáleně je nastaveno šifrování (pokud je přítomen čip TPM, nastaví služba autentizaci tak, aby byl použit). Obnovovací klíče jsou spravovány v cloudovém úložišti.

SW EMBASSY

Ostatní produkty jsou sjednoceny pod názvem EMBASSY a dají se vzájemně kombinovat. EMBASSY Trust Suite je balík pro podpoření bezpečnější autentizace uživatelů na počítačích vybavených TPM, biometrickou čtečkou nebo čtečkou karet smart card. Umožňuje spravovat hesla, nastavení TPM a zálohovat obnovovací klíče TPM. Podporuje přihlašování v doménách s využitím EMBASSY Authentication Server (ERAS), enterprise správu klíčů EMBASSY Key Management Server a vzdálenou administraci s EMBASSY

Remote Administration Server. Bezpečnější je i přihlašování přes VPN nebo do WIFI sítí při využití kombinace TPM a biometrických údajů (případně ještě certifikátů, uložených v TPM).

ERAS je nejkomplexnějším řešením od Wave. Kromě podpory všech funkcí popsaných u ostatních programů Wave sjednocuje řízení, monitorování a nastavení funkcí na jedno místo, jako snap-in modul Konzole Microsoft Management Console (MMC).

2.4 Tabulka využití TPM

Tabulka č. 2 porovnává jednotlivé programy podle funkcí TPM čipu, definovaných v části 1.4. Údaje, které nebyly přímo dohledatelné, jsou označené zkratkou NA[18].

SW	Svazování	Podepisování	Zapečetění	Zapečetěné podepisování	Podpora certifikátů
Linux	ano	NA	ano	NA	NA
BitLocker	ano	ne	ano	ne	ne
ThinkVantage	ano	ne	NA	ne	ano
HP ProtectTools	ano	ano	ano	ne	ano
McAfee EE	ano	ne	NA	ne	ne
Sophos	ano	ne	NA	ne	ne
Wave	ano	ne	ano	ne	ne

Tabulka č. 2: Funkce TPM, jak je využívají jednotlivé programy.

[18] Not Available - nedostupné

3 Využití TPM ve firmě

Firmy si na bezpečnosti dat dávají velice záležet. Každá větší společnost má povinné IT bezpečnostní politiky, především aby se zabránilo ohrožením zvenku, např. viry na CD nebo externích discích. Často existuje celý model bezpečnosti, který zahrnuje několik vrstev a chrání tak proti různým ohrožením zároveň. Takový model popíši na příkladu konkrétní společnosti.

3.1 Představení firmy

Společnost působící v oblasti financí a bankovnictví s více než 400 zaměstnanci, kde každý z nich má alespoň jeden počítač. Přes 200 z nich využívá přenosný počítač na cestách. Vzhledem k oblasti působení je zde extrémní důraz na bezpečnost dat.

3.1.1 Analýza aktuálního stavu IT

Ve firmě se používá software od Microsoft, aktuálně je na necelé čtvrtině počítačů nainstalován operační systém Windows XP Professional SP3, který pomalu končí a na všechny nové nebo přeinstalované počítače se nasazuje 64bitový Windows 7 Professional SP1. U serverů je situace podobná, jedná se o starší Windows Server 2003, který je nahrazován Windows Server 2008 R2. Výjimku tvoří zhruba dvě desítky přenosných počítačů Apple MacBook, na kterých běží buďto duální instalace MacOS X a Windows 7, či pouze MacOS X.

Běžný uživatel nemá povolen přístup k externím zařízením, nemůže si přehrát CD, DVD ani nemá přístup na flash disk, či jiná paměťová zařízení. Heslo do OS má minimální délku 8 znaků a je nutné použít kombinace s čísly, velkými a malými písmeny. Změna hesla je vyžadována každé tři měsíce. Uživatelé s notebookem mají navíc heslo pro zašifrovaný pevný disk. U uživatelů, kteří pracují s vysoce citlivými údaji, se pak šifruje i poštovní schránka a mají možnost důvěryhodně podepsat a odeslat šifrovaný e-mail.

Čip TPM se nepoužívá, není součástí procesu šifrování disku ani využíván žádnými dalšími programy, přestože je přítomen na všech NB a zhruba na polovině PC.

3.1.2 HW a cyklus obnovy

Pro stolní počítače je stanovena životnost 3 roky. Po této době je nahrazen novým modelem a ponechán jako náhradní nebo odprodán. Notebooky mají životnost kratší, a to 2 roky.

Hardware se tedy postupně sjednocuje. Veškeré nové stroje jsou značky Lenovo. U notebooků se jedná o řady ThinkPad T a X, které obsahují TPM čipy od výrobce Atmel. Pracovní stanice ThinkCentre M90p a M91p pak disponují TPM firmy ST Microelectronics.

Pokud ještě počítač nepřekročil stanovenou dobu životnosti, ale už nesplňuje SW požadavky (aktuální stav s Windows XP), je pouze přeinstalován SW na novější. Proto kompletní obměna všech starších PC za nové proběhne odhadem během roku 2013.

3.1.3 Software

Na stolních počítačích není žádná dodatečná ochrana proti případnému útočníkovi, jelikož zůstávají v budově střežené kamerovým systémem, dveřmi s přístupem na čipovou kartu a ochrankou. Proti útokům tedy chrání pouze integrovaný firewall systému Windows a ESET NOD32 Antivirus. Internetová komunikace je navíc chráněna HW firewallem.

McAfee Endpoint Encryption

Na šifrování pevných disků se používá software McAffee Endpoint Encryption. Šifrován je celý disk a heslo je vyžadováno před začátkem bootování operačního systému. Management a správa strojů a uživatelů je řešen přes vlastní EE Server. Při instalaci nového PC se musí ve firemní síti nejdříve synchronizovat nastavení šifrování (je nastavena síla šifrování, typ autentizace uživatele, konkrétní uživatel je přiřazen k danému stroji a jsou určeny disky k zašifrování). Rozšifrovat disk např. v případě poruchy stanice lze za pomoci vygenerovaného kódu přes management na EES. Pevný disk je šifrován pouze u přenosných počítačů. V Encryption Manager je každému počítači přiřazen konkrétní uživatel, takže do systému se může přihlásit jen majitel NB a administrátoři. Firma plánuje přechod na aktuálně nejnovější verzi, která podporuje i operační systém MacOS.

Cisco VPN Client

Uživatelé pracující z domova potřebují přístup na firemní e-mail, intranet a síťové aplikace. K tomu používají šifrované spojení VPN pomocí SW od společnosti Cisco, příp. Citrix. Znamená to pro ně další přihlašovací heslo a používání speciálního programu.

Lumension Endpoint Protection

Zabraňuje připojení jakýchkoliv USB zařízení na uživatelském PC. Povolovat lze selektivně uživatelům buď pouze konkrétní zařízení, nebo celou skupinu (např. skenery). Klient Lumension je instalován na každém PC, správa probíhá síťově ze serveru.

3.1.4 Další zabezpečení

Čtečky otisků prstů slouží ke spárování uloženého otisku s uživatelským heslem. Program pouze vyplní za uživatele heslo, pokud se otisk shoduje s uloženým, nepoužívá se žádný vyšší stupeň zabezpečení.

K přihlášení do domény na firemní WiFi síti je nutný certifikát, který je automaticky nainstalován při prvním přihlášení uživatele přes kabelové připojení.

3.2 Návrh na změnu zabezpečení s využitím TPM

Čipy jsou dostupné ve všech spravovaných NB a na všech nově dodávaných stolních PC, což značně snižuje náklady na případné nasazení ve firmě. Aktuálně lze spustit podporu TPM na přenosných PC a to v souvislosti s šifrováním pevného disku. TPM by sloužilo jako úložiště soukromých klíčů a šifrovací procesor by snižoval zátěž CPU. Svazování s konkrétní platformou by přidalo dodatečné zabezpečení.

Využití jako chráněné úložiště je možné použít např. pro certifikáty šifrování pošty, které jsou aktuálně instalované na pevném disku.

3.2.1 Dostupná řešení a jejich popis

Řešení č. 1 Přidat ověření pomocí TPM v McAfee Endpoint Encryption

Pro popsanou situaci se jedná o nejjednodušší řešení, jak finančně, tak složitostí. Systém, který je aktuálně v provozu, se osvědčil ve spolupráci s ostatními programy a zabezpečeními a uživatelé jsou na něj zvyklí. Z pohledu uživatele by se nic nezměnilo a kompatibilita s ostatními programy by zůstala zachována. McAfee EE podporuje ověřování platformy pomocí dat bezpečně uložených uvnitř TPM. Při změně HW konfigurace nebude proces ověření platformy úspěšný a systém nenastartuje. Součástí SW je možnost centrálně zálohovat klíče pro případ poruchy čipu.

Pozn. McAfee uvádí podporu pouze pro TPM čipy výrobce Infineon, jiné otestovány nejsou. Lenovo dodává PC a NB s čipy ST Microelectronics, resp. Atmel, takže kompatibilita není zaručena.

Řešení č. 2 Přechod na Windows 7 Enterprise a nástroj BitLocker

Je náročnějším řešením z časového hlediska. Množství práce a reinstalace jednotlivých PC/NB vyžaduje v průměru cca jeden den, kdy je uživatel bez počítače. Nejvyšší edice Windows je k dispozici v rámci již aktivní smlouvy s Microsoft (typ Enterprise). Nejrychlejší přechod nabízí využití možnosti upgrade na vyšší edici Windows při zachování dat, aplikací a nastavení. Informace a záložní klíče TPM by byly ukládány do AD. Pro vyšší efektivitu a vzdálené nastavení by bylo nutné napsat vlastní skripty pro utilitu *manage-bde.exe*.

Řešení č. 3 Přechod na kompletní systém jiného výrobce

Kompletní systém zahrnující šifrování disku, ověření uživatele, případně i antivirus a antispyware. Ověřování a šifrování by využívalo TPM. Řešení se dělí na dvě části – lze spojit s řešením č. 2 a napojit SW na nástroj BitLocker nebo použít vlastní šifrovací SW dané firmy.

První možnost by byla méně náročná na pořizovaný produkt, ale celkově se situace vyrovná (nutnost reinstalace Windows na edici Enterprise). Šifrování disku by zařídil BitLocker, ale veškeré nastavení a správa by bylo centrální díky SW třetí strany, např. Wave for BitLocker Management (viz část 2.3.3).

Druhou možností je nákup specializovaného produktu od společnosti Wave nebo Sophos, který by nahradil stávající šifrování McAfee. SW Safeguard Easy by byl řešením od Sophosu a kombinace programů z řady EMBASSY v případě společnosti Wave.

Řešení č. 4 Instalovat Lenovo ThinkVantage Client Security Solution

Software, který nabízí „doplňkové" zabezpečení pro hesla a otisky prstů a uživatel může zjistit aktuální stav několika bezpečnostních prvků, zejména čipu TPM. SW nelze nainstalovat centrálně, proto by se uživatelům instaloval jednotlivě s krátkým vysvětlením funkčnosti. Toto řešení nabízí funkce, které obecně neposílí celkové zabezpečení systému, proto by instalace měla být pouze pro vybrané uživatele, kteří využívají certifikáty s privátními klíči a případně pro další, kteří by měli zájem využívat otisky prstů a ukládání hesel. Náklady z finančního hlediska zahrnují pouze práci strávenou instalací, samotný program je pro majitele strojů Lenovo k dispozici zdarma.

Řešení č. 5 Úložiště v TPM využít pro certifikáty a/nebo ověření přístupu do sítě

Podpora MS-CAPI[19], PKCS #11[20] a #12[21] zaručuje kompatibilitu s běžnými kryptografickými rozhraními a stávajícími certifikáty. Uložení do TPM je bezpečnější, nelze je přenést s pevným diskem do jiného počítače. Stejně tak by se změnilo úložiště pro certifikát přihlášení k bezdrátové síti.

Přístup do VPN sítě lze zjednodušit, aby nemuselo být zadáváno další heslo – pokud je přihlášení do systému zabezpečeného pomocí TPM s heslem úspěšné, znamená to, že s počítačem nikdo nemanipuloval a uživatel je důvěryhodný.

---

[19] Microsoft CryptoAPI – je API integrované v systému Windows, podporuje programy používající (de)šifrování, použití certifikátů, veřejné i symetrické klíče a obsahuje generátor náhodných čísel.

[20] Public-Key Cryptography Standard #11: Cryptographic Token Interface Standard – specifikace API pro zařízení, která ukládají kryptografické informace a provádějí kryptografické operace. [32]

[21] Public-Key Cryptography Standard #12: Personal Information Exchange Syntax Standard – standard pro ukládání a přenášení uživatelských certifikátů, včetně privátních klíčů. [33]

3.2.2 Výběr řešení

Postup při výběru řešení záleží na cílech dané firmy, především na rozhodnutích týkajících se stupňů bezpečnosti. TPM by ideálně mělo mít pro firmu dva základní přínosy a to zjednodušení přihlašování pro uživatele a posílení stávajícího způsobu zabezpečení. Pokud nelze zjednodušit proces přihlašování uživatelů, měl by mít stejný počet kroků jako dosud.

Kombinace více řešení zaručí využití TPM ve více oblastech než je pouze šifrování HDD. Pro posuzovanou firmu bude nejefektivnější nasazení řešení č. 1, případně č. 2. Jako doplňující funkčnost lze potom pro vybrané uživatele zvolit řešení č. 4. U řešení č. 3 by se kvůli finanční náročnosti muselo zvážit, zda se vyplatí, vzhledem ke zvýšené bezpečnosti.

3.2.3 Postup nasazení

Nasazení bude vždy popsáno v krocích, které na sebe bezprostředně navazují. Součástí je hrubý časový odhad nasazení. První bod bude stejný u všech řešení:

- aktivace TPM v systému BIOS

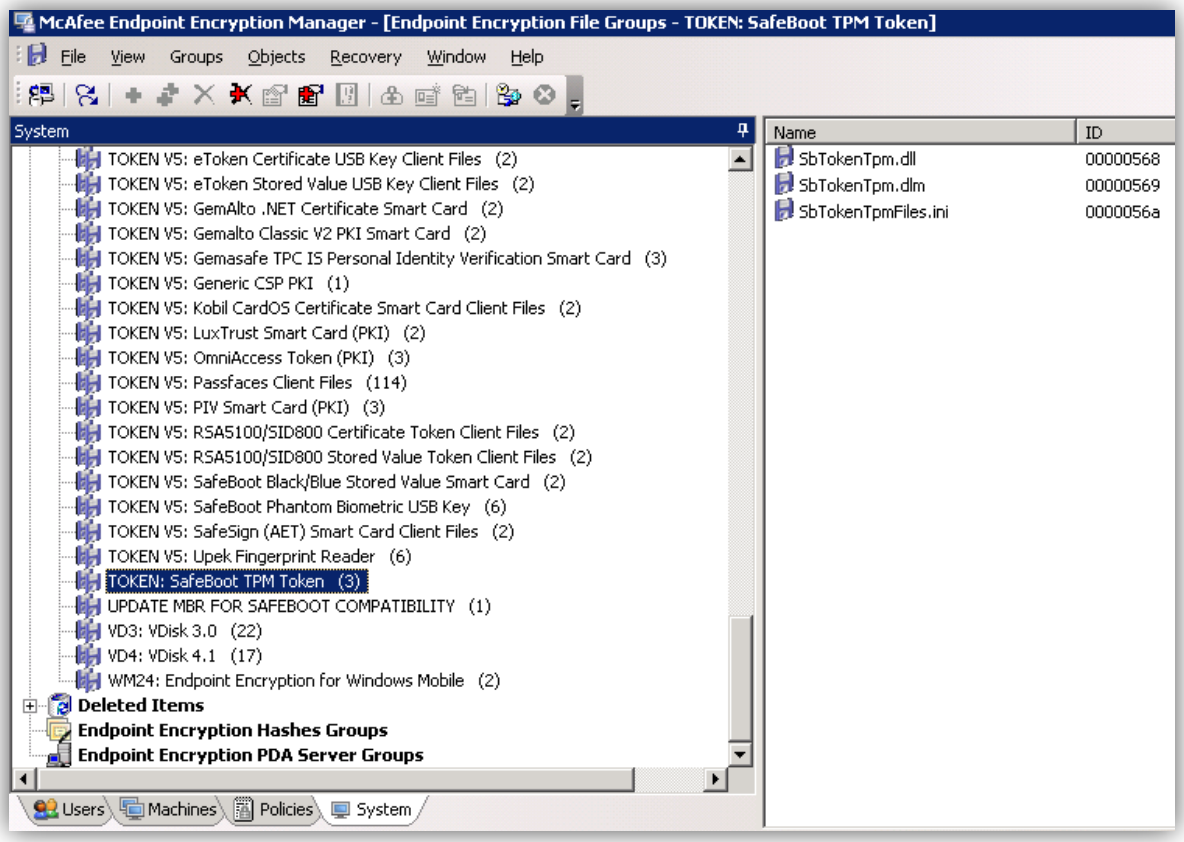
Řešení č. 1 Přidat ověření pomocí TPM v McAfee Endpoint Encryption

- převzetí vlastnictví čipu ve Windows
- nastavení balíčku s tokenem TPM ve správci EE Manager, synchronizace (viz obrázek č. 10)
- doškolení uživatelů (na přihlašovací obrazovce bude nově možnost vybrat přihlášení s tokenem TPM)

Toto řešení se v praxi bohužel ukázalo jako nefunkční z důvodu jiného výrobce čipu TPM u počítačů Lenovo. McAfee uvádí kompatibilitu otestovanou pouze s čipy Infineon (tomu odpovídá i použití SafeBoot šifrování u počítačů HP[22]).

Odhadovaná doba nasazení: 15 minut/uživatel

[22] HP instaluje do svých strojů pouze čipy výrobce Infineon.



Obrázek č. 10: Prostředí McAfee EE Manager – soubory přihlašovacího tokenu TPM.

Řešení č. 2 Přechod na Windows 7 Enterprise a nástroj BitLocker

- reinstalace/upgrade OS na edici Enterprise
- převzetí vlastnictví čipu ve Windows, uložení obnovovacího klíče do AD
- nastavení nástroje BitLocker (lze automaticky vynutit skupinovou politikou domény)
- spuštění šifrování
- doškolení uživatelů (jiné heslo před startem OS, jiná obrazovka)

Odhadovaná doba nasazení: 2 hodiny/uživatel při upgrade, jinak cca 1 den/uživatel

Řešení č. 3 Přechod na kompletní systém jiného výrobce

- zprovoznění serveru a centrálního managementu
- v případě nástroje BitLocker další postup jako u řešení č. 2, ale již centrálně ovládáno

- v případě SW společnosti Wave lze vše provést centrálně, od převzetí vlastnictví, až po nastavení a spravování šifrování

Odhadovaná doba nasazení: instalace a testování systému min. 1 týden, potom 30 minut/uživatel (v případě nástroje BitLocker +2 hodiny/uživatel)

Řešení č. 4 Instalovat Lenovo ThinkVantage Client Security Solution

Předpoklad: v systému BIOS je povolena čtečka otisků prstů, ovladače ThinkVantage Fingerprint Software jsou nainstalované ve Windows.

- převzetí vlastnictví čipu ve Windows
- lokální instalace Client Security Solution
- kontrola stavu zabezpečení přes funkci Audit (viz obrázek č. 11)
- oprava, resp. povolení funkcí podle výsledků Auditu
- převod uživatelských certifikátů do čipu TPM
- zaškolení uživatelů, jak používat hesla, příprava návodu na nastavení a používání (pro vystavení na intranet)

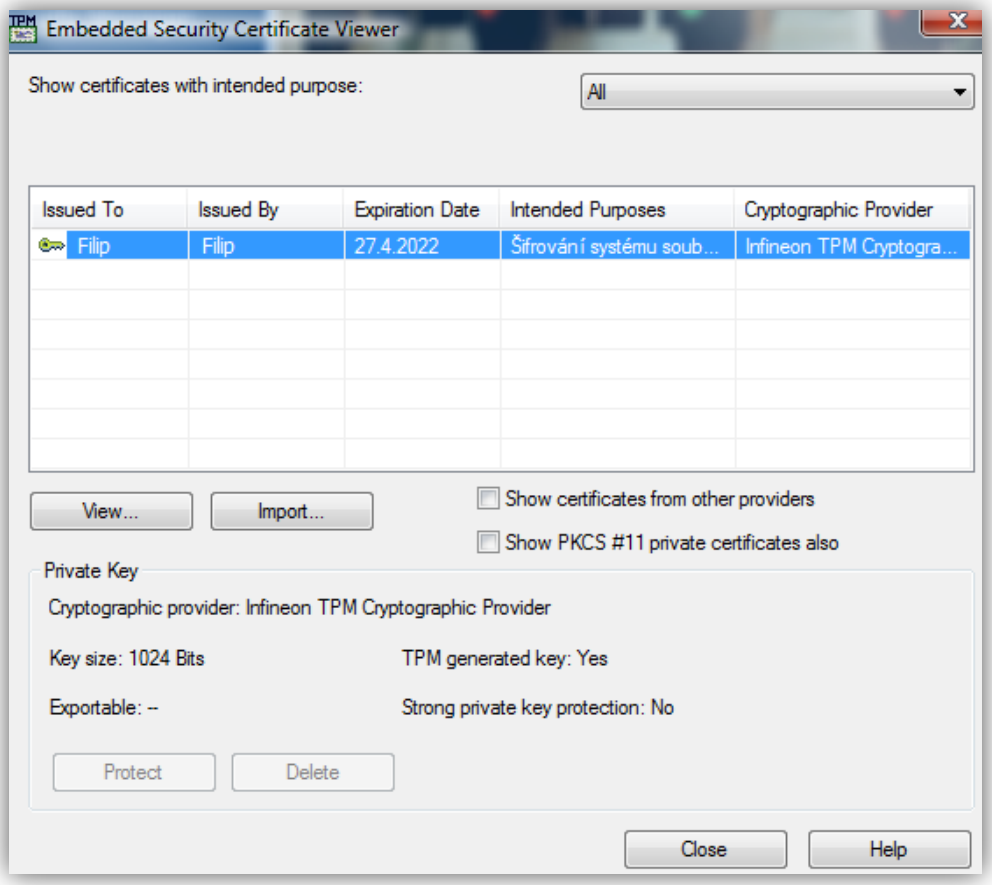
Odhadovaná doba nasazení: 15 minut/uživatel

Obrázek č. 11: Funkce Audit v programu Client Securiy Solution.

Řešení č. 5 Úložiště v TPM využít pro certifikáty a/nebo ověření přístupu do sítě

- lokální instalace balíku Infineon TPM Professional Package
- převzetí vlastnictví čipu v programu
- převod uživatelských certifikátů a přihlašovacích údajů k VPN do úložiště čipu TPM (viz obrázek č. 12)

Odhadovaná doba nasazení: 15 minut/uživatel



Obrázek č. 12: Import a správa certifikátů v programu Infineon TPM Professional Package.

Závěr

Silné heslo samo o sobě nestačí, ani v kombinaci s kvalitním šifrováním a privátní klíče z šifrovacího algoritmu je také nutné někde uložit. To je oblast, kterou ovládá čip TPM a kde má pořád široké možnosti využití. Kritika je ovšem silná a zdá se, že uživatelé na internetových fórech a diskuzích se dělí na dvě skupiny – jedni, kteří zatím ani nevěděli, že čip existuje a snaží se zjistit o něm další informace a druzí, kteří se snaží první skupinu odradit od používání z mnoha důvodů, které jsem vysvětlil v kapitole věnované kritice. V dnešní době není zvláštností, že nově uvedený bezpečnostní prvek je pokořen v řádu hodin, případně dnů. Starší verze čipu TPM už prolomena byla, sice za dosti specifických podmínek, ale zpochybnit nebo zamlčet to nelze. Samotná organizace TCG ve svých dokumentech jasně uvádí, že neručí za 100% zabezpečení. Ani nemůže, když značná část výsledné podoby čipu je ovlivněna výrobcem.

U dnešních šifrovacích programů, které používají AES s 256bitovým klíčem je pro útočníka v podstatě nemožné získat klíč v rozumném čase. Na druhou stranu privátní klíč bývá uložen mimo zašifrovanou oblast (bootovací oddíl nebo „boot loader“), což znamená riziko.

Na začátku práce jsem popsal základní architekturu TPM a obecně definoval funkce čipu. V další podkapitole jsem popsal aktuální situaci na trhu – kteří výrobci a v jakých kategoriích nasazují čipy TPM (včetně výrobce samotného čipu, pokud byl údaj k dispozici). Následně jsem vysvětlil jednotlivé zásady, které TCG doporučuje dodržovat všem, jak firmám při nasazování TPM, tak vývojářům při navrhování aplikací pro TPM. Tyto zásady zároveň TCG chápe a prezentuje jako best practices. Dále jsem shrnul jednotlivé kritické názory proti TPM řešení a uvedl, na čem stojí. V kapitole věnované SW jsem představil a porovnal programy ve třech kategoriích – s podporou TPM přímo v OS, nástroje předinstalované výrobci PC/NB a komerční programy. V praktické části jsem se zaměřil na konkrétní firmu, aktuální stav IT a uvedl programy, které se používají k zabezpečení stanic. Následně jsem navrhl několik řešení, která lze aplikovat u dané firmy. Nakonec jsem naznačil, jak lze vybraná řešení ve firmě zavést. Cíle práce, které jsem naznačil v úvodu tak považuji za splněné.

Rozšíření tématiky např. v diplomové práci je možné v několika oblastech. Práce by mohla analyzovat rozsáhlou problematiku příkazů TPM spolu s dostupným API pro tvorbu

aplikací s podporou TPM, ideálně s navržením aplikace pro konkrétní použití. Jiné možné téma by mohlo obsáhnout velmi podrobně veškeré nalezené argumenty proti řešení TPM a pokusit se je dokázat nebo vyvrátit vytvořením sady testů, které by se daly spustit na čipech různých výrobců. Po spuštění testů na různých platformách by se data analyzovala a výsledky porovnávaly.

Na základě informací zjištěných při psaní této práce si myslím, že čip TPM může velmi dobře fungovat jako další ochranný prvek, který zvýší bezpečnost jak na osobním počítači, tak ve firmě. Pro případného útočníka je to další, a ne zrovna triviální, překážka navíc. To vše za předpokladu, že je použit regulérně, tzn. na základě zásad TCG („best practices“). TPM čip by si zasloužil více propagace, testování, ukázek praktického použití a především nasazení i do střední třídy NB/PC. Pak by se dalo o jeho kvalitách, či případných nedostatcích diskutovat v širším spektru a povědomí uživatelů by se rozrostlo o další bezpečnostní prvek.

Příloha A: Terminologický slovník

Termín anglicky (zkratka)	Termín česky	Význam
Attestation Identity Key (AIK)	Klíč atestační identity	Důvěryhodný klíč, uložený v non-volatilní paměti TPM. Je používán k podepisování PCR hodnot.
Binding	Svazování	Funkce TPM, pro zašifrování se použije veřejný a soukromý klíč, přičemž soukromý zůstává chráněn v úložišti TPM.
Digital Rights Management (DRM)	Správa digitálních práv	Systém pro ochranu digitálního obsahu, především multimédií. Může být zastoupen mnoha různorodými technologiemi.
Endorsement Key (EK)	-	Jedinečný klíč, který se vygeneruje a uloží v TPM již při výrobě. Zůstává uvnitř čipu ve stejné podobě po celou dobu jeho životnosti.
Microsoft CryptoAPI (MS-CAPI)	-	API pro podporu kryptografických operací v programech, integrované v systému Windows.
Owner Auth Secret (OAS)	-	Autorizační data vlastníka – záznam vzniká při převzetí vlastnictví čipu.
Platform Configuration Register (PCR)	Konfigurační registr platformy	Při šifrování uložená hodnota HW nebo SW prvku platformy, která se porovnává s aktuální před dešifrováním.
Protection Profile	Profil ochrany	Podrobně definuje bezpečnostní prvky TPM. Je součástí specifikačních dokumentů, doplňuje hlavní specifikaci.
Public-Key Cryptography Standard #11 (PKCS #11)	-	API pro zařízení, která ukládají kryptografické informace a provádějí kryptografické operace.
Public-Key Cryptography Standard #12 (PKCS #12)	-	Standard pro ukládání a přenášení uživatelských certifikátů, včetně privátních klíčů.
Sealed-Signing	Zapečetěné podepisování	Spojení svazovacích operací s konkrétním stavem platformy pomocí PCR hodnot.

Sealing = Sealed-Binding	Zapečetění	Spojení podepisovacích operací s konkrétním stavem platformy pomocí PCR hodnot.
Self-encrypting Drive (SED)	-	Úložiště, které je schopné automatického transparentního HW šifrování.
Signing	Podepisování	Funkce TPM, na základě zprávy se vytváří klíč pro vygenerování podpisu.
Storage Root Key (SRK)	-	Kořenový klíč, sloužící jako základ šifrování. Je uložený v non-volatilní paměti TPM a čip nikdy neopouští.
TCG Compliance	-	Označení splnění požadavků specifikace.
TCG Software Stack (TSS)	-	Souhrn komponent pro podpora aplikací, které budou TPM používat.
TCG technology	TCG technologie	Obecné označení pro standardy vyvinuté TCG, v textu se většinou vztahuje konkrétně na TPM.
Trusted Computing (TC)	-	Práce s platformou, která je důvěryhodná, což je zajištěno pomocí TCG technologií.
Trusted Computing Group (TCG)	-	Neziskové sdružení vytvořené za účelem zavedení a zlepšení standardů v oblasti bezpečnosti IT.
Trusted Computing Platform Alliance (TCPA)	-	Dřívější název skupiny TCG.
Trusted Platform	Důvěryhodná platforma	Platforma obsahující bezpečnostní čip TPM, který je aktivován a bylo převzato vlastnictví. Zaručuje, že s platformou nebylo nijak manipulováno.
Trusted Platform Module (TPM)	Modul důvěryhodné platformy	Samostatný čip, integrovaný na základní desce, schopný provádět kryptografické operace a bezpečně skladovat šifrovací klíče.

Příloha B: Seznam literatury

[1] Trusted Computing Group [online]. © 2012 [cit. 2012-03-14]. Dostupné z: http://www.trustedcomputinggroup.org/

[2] ZEMAN, Vlastimil. *Trusted Platform Module a jeho emulácia*. Brno, 2007. Bakalářská práce. Masarykova univerzita, Fakulta informatiky.

[3] MOKOŠ, Ondřej. *Trusted Platform Module a jeho emulace*. Brno, 2009. Bakalářská práce. Masarykova univerzita, Fakulta informatiky.

[4] MÁLEK, Ondřej. *Využití modulu důvěryhodné platformy pro podporu systému TrueCrypt*. Brno, 2009. Diplomová práce. Masarykova univerzita, Fakulta informatiky.

[5] STETSKO, Andriy. *Principy a využití modulu důvěryhodné platformy*. Brno, 2007. Diplomová práce. Masarykova univerzita, Fakulta informatiky.

[6] VILA, Elior a Plamenka BOROVSKA. Data protection utilizing trusted platform module. In: *CompSysTech '08 Proceedings of the 9th International Conference on Computer Systems and Technologies and Workshop for PhD Students in Computing* [online]. 2008 [cit. 2012-03-08]. Dostupné z: databáze ACM Digital Library.

[7] TRUSTED COMPUTING GROUP. *TCG Specification Architecture Overview* [online]. 2.8.2007 [cit. 2012-03-09]. Dostupné z: http://www.trustedcomputinggroup.org/resources/tcg_architecture_overview_version_14

[8] TRUSTED COMPUTING GROUP. *Trusted Platform Module (TPM) Summary* [online]. © 2012 [cit. 2012-05-02]. Dostupné z: http://www.trustedcomputinggroup.org/resources/trusted_platform_module_tpm_summary

[9] TRUSTED COMPUTING GROUP. *Protection Profile PC Client Specific Trusted Platform Module TPM Family 1.2* [online]. Květen 2011 [cit. 2012-04-24]. Dostupné z: http://www.trustedcomputinggroup.org/resources/tpm_12_protection_profile

[10] SAMS, Brad. HP is working on x86 Windows 8 tablet, rough render exposed. In: *Neowin* [online]. Duben 2012 [cit. 2012-05-04]. Dostupné z: http://www.neowin.net/news/hp-is-working-on-x86-windows-8-tablet-rough-render-exposed

[11] LEBLANC, Brandon. Announcing the Windows 8 Editions. In: Blogging Windows [online]. Duben 2012 [cit. 2012-05-05]. Dostupné z: http://windowsteamblog.com/windows/b/bloggingwindows/archive/2012/04/16/announcing-the-windows-8-editions.aspx

[12] INTEL CORPORATION. *Going Beyond Exceptional Computing Performance* [online]. 2011 [cit. 2012-05-01]. Dostupné z: http://download.intel.com/embedded/technology/325564.pdf

[13] TRUSTED COMPUTING GROUP. *TCG Design, Implementation, and Usage Principles (Best Practices)* [online]. Únor 2011 [cit. 2012-03-15]. Dostupné z: http://www.trustedcomputinggroup.org/resources/tcg_design_implementation_and_usage_principles_best_practices

[14] SADEGHI, Ahmad-Reza, Marcel SELHORST, Christian STÜBLE, Christian WACHSMANN a Marcel WINANDY. TCG inside?: a note on TPM specification compliance. In: *STC '06 Proceedings of the first ACM workshop on Scalable trusted computing* [online]. 2006 [cit. 2012-03-04]. Dostupné z: databáze ACM Digital Library.

[15] TrueCrypt - Free Open-Source On-The-Fly Disk Encryption Software for Windows 7/Vista/XP, Mac OS X and Linux - FAQ. *TrueCrypt - Free Open-Source On-The-Fly Disk Encryption Software for Windows 7/Vista/XP, Mac OS X and Linux* [online]. 18.4.2011 [cit. 2012-03-11]. Dostupné z: http://www.truecrypt.org/faq

[16] VOGEL, Lutz a Benjamin STEPHAN. Trusted Computing [online]. 2009 [cit. 2012-04-20]. Dostupné z: http://vimeo.com/5168045

[17] HOUSER, Pavel. Zranitelnost v TPM je hrozivá. In: SecurityWorld [online]. 2010 [cit. 2012-04-26]. Dostupné z: http://securityworld.cz/securityworld/zranitelnost-v-tpm-je-hroziva-2290

[18] Trusted Computing Group - Solutions - Data Protection. *Trusted Computing Group - Home* [online]. © 2012 [cit. 2012-03-15]. Dostupné z: http://www.trustedcomputinggroup.org/solutions/data_protection

[19] Trusted Computing Group - TCG Members. *Trusted Computing Group - Home* [online]. © 2012 [cit. 2012-03-15]. Dostupné z: http://www.trustedcomputinggroup.org/about_tcg/tcg_members

[20] Windows Trusted Platform Module Management Step-by-Step Guide. In: *Microsoft TechNet Library* [online]. © 2012 [cit. 2012-02-07]. Dostupné z: http://technet.microsoft.com/en-us/library/cc749022(WS.10).aspx

[21] Best Practices for BitLocker in Windows 7. In: *Microsoft TechNet Library* [online]. © 2012 [cit. 2012-02-20]. Dostupné z: http://technet.microsoft.com/en-us/library/dd875532(v=ws.10).aspx

[22] Optimizing Client Security by Using Windows Vista. In: *Microsoft TechNet Library* [online]. © 2012 [cit. 2012-02-20]. Dostupné z: http://technet.microsoft.com/en-us/library/bb735277.aspx

[23] Backing Up BitLocker and TPM Recovery Information to AD DS. In: *Microsoft TechNet Library* [online]. © 2012 [cit. 2012-02-20]. Dostupné z: http://technet.microsoft.com/en-us/library/dd875529(v=ws.10).aspx

[24] BitLocker Command-line Tools. In: *Microsoft TechNet Library* [online]. © 2012 [cit. 2012-02-20]. Dostupné z: http://technet.microsoft.com/en-us/library/ee706522(v=ws.10).aspx

[25] OIAGA, Marius. Windows 8 Secure Boot. In: *Softpedia* [online]. 2011 [cit. 2012-03-15]. Dostupné z: http://news.softpedia.com/news/Windows-8-Secure-Boot-221460.shtml

[26] Secured Boot and Measured Boot: Hardening Early Boot Components Against Malware. In: MICROSOFT. *Dev Center - Hardware* [online]. 2011 [cit. 2012-03-15]. Dostupné z: http://msdn.microsoft.com/en-us/library/windows/hardware/br259097

[27] HP ProtectTools - keep data, networks and communications protected from threats. HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P. *HP - United States | Laptop Computers, Desktops, Printers, Servers and more* [online]. © 2011 [cit. 2012-03-15]. Dostupné z: http://h20331.www2.hp.com/Hpsub/cache/281822-0-0-225-121.html

[28] MCAFEE, Inc. *McAfee Endpoint Encryption for PC-5.2.9*: *Administration Guide* [online]. 2007 [cit. 2012-03-15]. Dostupné z: https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/23000/PD23125/en_US/EEPC529_Admin_Guide.pdf

[29] UTIMACO SAFEWARE AG. *Embedded Security*: *Trusted Platform Module Technology Comes of Age* [online]. 2005 [cit. 2012-03-15]. Dostupné z: http://www.computerworld.com/pdfs/Utimaco_EmbeddedWP706.pdf

[30] Data Encryption Technology, Encrypt Drives, Files and Folders | Sophos. *Antivirus, Endpoint, Disk Encryption, Email and Web Security | Sophos* [online]. © 1997-2012 [cit. 2012-03-15]. Dostupné z: http://www.sophos.com/en-us/products/encryption.aspx

[31] Products | Wave Systems Corp. *Wave Systems Corp.* [online]. © 1997-2012 [cit. 2012-03-15]. Dostupné z: http://www.wave.com/products/

[32] EMC CORPORATION. PKCS #11: Cryptographic Token Interface Standard. In: *RSA Laboratories* [online]. © 2012 [cit. 2012-05-06]. Dostupné z: http://www.rsa.com/rsalabs/node.asp?id=2133

[33] EMC CORPORATION. PKCS #12: Personal Information Exchange Syntax Standard. In: *RSA Laboratories* [online]. © 2012 [cit. 2012-05-06]. Dostupné z: http://www.rsa.com/rsalabs/node.asp?id=2138

Příloha C: Seznam obrázků a tabulek

Seznam obrázků

Seznam tabulek