

Filip Eichenmann

TPM – Trusted Platform Module

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 výrobcí přenosných počítačů pro podporu čipu TPM a popsat využití TPM s programy pro šifrování pevných disků. Následovat bude návrh, jak by se mohlo využít funkcí TPM, jak při zachování současně používaných programů, tak s použitím nového software.

velmi dobře (2)

Celkové zhodnocení práce a případné otázky pro diskusi (případně na další samostatný list):

RNDr. Radomír Palovský, CSc.

Podpis oponenta bakalářské práce

Posudek na bakalářskou práci Filipa Eichenmanna s názvem TPM – Trusted Platform Module.

RNDr. Radomír Palovský, CSc.

Bakalář se v práci věnuje vlastnostem a fungování chipu TPM. Práce je dosti pečlivě zpracována, vývody jsou dobře zdokumentovány odkazy na literaturu. V práci jsou zpracovány charakteristiky funkcionality i kritiky celého přístupu přes TPM. V závěru podává bakalář návrh na změnu bezpečnostní modelu firmy, která má většinu počítačů osazenou moduly TPM.

Bezpečnost informací a zvláště kryptografické modely jsou velmi zvláštní podoborem IT systémů. Stačí jedna důležitá slabina a bezpečnost může být ohrožena v mnohem větším rozsahu než by slabina z prvního pohledu napovídala. Bezpečnost je v podstatě vždy obchod s důvěrou, a pokud slabina důvěru zásadně poruší, je vnímání bezpečnosti ztraceno. Bakalář v části 1.8 se věnuje kritice, které se technologií TPM a TCG dostalo. Část z nich je závažná koncepční, jako je kompatibilita čipů, kritiky správy klíčů a zranitelnost TPM při práci administrátora. Vzhledem k tomu, že v poslední části bakalář podává návrh na změnu modelu fungování firmy s tím, že by přešla na využití modulů TPM instalovaných v počítačích bylo by žádoucí, aby bakalář se věnoval i vztahu nedostatků návrhu TPM modulů a této konkrétní implementace a teď odpověděl otázky:

1. Jak se projeví nedostatky modulu TPM v tomto konkrétním nasazení a jsou tyto slabiny pokryty jinými prostředky bezpečnostního modelu firmy? (např. ve vztahu k různým zařízením s různými TPM chipy, k administraci systémů zvláště notebooků.)
2. Má vůbec nasazení zabezpečení s využitím modulu TPM reálné zvýšení bezpečnosti proti současnému využití čistě softwarového bezpečnostního modelu a jaké?

18. června 2012

RNDr. Radomír Palovský, CSc.