USB trezory aneb jak Pašák chránil data

Pašáky nazýváme v našem seriálu „odborníky, co všechno ví, a hned jdou na věc“. Uvidíme, jak se jim podařilo zničit původně velice užitečný a bezpečný flash disk. USB flash disky jsou rozšířené a oblíbené, neboť se masivně používají pro každodenní operativní přenos dat. Časem je asi nahradí SSD disky, ale než se zlevní, bude to ještě pěkných pár let trvat. Díky rozšířenosti a oblíbenosti se flash disky staly cílem virů a malware všeho druhu, stejně jako tomu bylo v dávných časech u disket. A všechno se znovu opakuje dokolečka. Diskety byly největším přenašečem a distributorem virů a USB flash disky je následují. Nemohou dosáhnout takového „zamoření“ jako diskety, ale jen díky tomu, že diskety byly ve své době jediným médiem na přenos dat, zatímco dnes je více alternativ, a zejména díky tomu, že antiviry jsou běžnou součástí počítačů. Po antivirech se začaly diskety také šifrovat – jako média nebo soubory na nich, a to samé se děje s flash disky. Zákonitě, neboť i tato média se ztrácí nebo v horším případě kradou.

Obr. 1 Příklady fyzicky velice odolných flash sticků (voda, oheň, náraz). Z hlediska autorovy zkušenosti je nejlepší prostřední (32 GB); bohužel nemají ani hadwarové šifrování ani klávesnici.

Bezpečný USB flash disk

Co bychom očekávali od bezpečného flash disku? Za prvé, když ho někdo náhodně najde nebo zcizí, aby z něj nezískal data. To je z technického hlediska, jak uvidíme dále, to nejjednodušší, co se má a může zajistit, řeklo by se – téměř triviální záležitost. Postačí data, která se na disk ukládají, šifrovat. To lze dvěma způsoby; za prvé šifrovat soubory na počítači a teprve šifrované soubory ukládat na flash disk. To má svá plus i mínus. Výhodou je, že disk můžeme nosit všude k přátelům, nemusíme nikde v cizím prostředí vkládat náš šifrovací klíč a na „flashku“ si můžeme ukládat otevřená i šifrovaná data podle své potřeby. Z toho se odvíjí použití zejména pro osobní potřeby, kdy data vlastní uživatel a nikoli organizace, která by ráda rozhodovala, jak mají být její data, potulující se na flash discích, chráněna. Postačí nám tedy nějaký souborový šifrovací program pro šifrování a dešifrování souborů a obyčejný flash disk.

O stupínek výše

Organizace půjde možná jinou cestou, a to za prvé nějakým opatřením proti šíření virů pomocí těchto disků a za druhé opatřením proti vynášení dat mimo počítače organizace. Ale i zde je nutné chránit data při cestách zaměstnanců, čili je nutné mít data na flashkách šifrovaná. V tomto případě však není jiné cesty, než šifrovat celý flash disk, protože při ukládání dat nesmí rozhodovat zaměstnanec, která data jsou nebo nejsou potřeba šifrovat. Čili musí se šifrovat celý disk, a to tzv. na pozadí (on-the-fly), tedy transparentně z hlediska počítače. Toto šifrování nemůže být děláno softwarově na počítači, protože zaměstnanec by ho mohl vypnout a předělat si šifrovaný disk na nešifrovaný. K tomuto účelu je tedy vhodné použít flash disky, které mají šifrování zabudováno přímo v sobě, tj. ve svém hardwaru. Takových USB disků je na trhu celá řada, a některé dokonce s certifikátem FIPS 140-2 (nebo nově už FIPS 140-3) amerického úřadu NIST. Takové flashky se mohou používat ve státní správě USA. Pokud hovoříme o státní správě, kde se pohybují citlivé informace (ale ještě nehovoříme o utajovaných), i počítače a počítačové sítě státní správy musí mít definováno určité bezpečnostní prostředí (opět certifikované). Čili je tu zajištěna bezpečnostní kultura, a to, že na počítačích, kde se k flashce zadávají hesla (PINy, passwordy, klíče), nejsou viry nebo malware, odchytávající tato hesla. Vkládání hesel přes klávesnici počítače je proto v tomto prostředí možné považovat za bezpečné. Flash disk je uvnitř organizace v bezpečném prostředí a pokud se ocitne mimo, jsou data na něm šifrovaná. Klíč k datům je uložen v hardware flash disku a je „dostupný“ pouze po zadání hesla, které zná zaměstnanec. Zde je také vidět, že zaměstnanec organizace nesmí mít možnost použít flash disk mimo bezpečné prostředí organizace (třeba doma), neboť při vkládání hesla v nezabezpečeném počítači by mohlo dojít k jeho odchycení útočníkem. Útočník by po získání flash disku mohl vystupovat jako oprávněný uživatel a zkopírovat všechna data. Aby byl flash disk nepoužitelný mimo organizaci, je možné technicky zajistit, i když to není triviální záležitost. Zdá se tedy, že poslední baštou útočníka je flash disk sám o sobě, pokud ho získá. To se může snadno stát na cestě zaměstnance domů nebo na jiné pracoviště organizace, v hotelu, na letišti apod. Nemusí jít ani o krádež, ale o prostou ztrátu, což se skutečně také dost často stává. V případě, že to nastane, měla by bezpečnostní opatření zajistit, že nálezce nebo útočník nemůže data získat; to je také účelem hardwarově šifrovaného flash disku a odráží se nepříjemně v jeho ceně.

Certifikovaný zmetek

Nedávno byl odhalen jeden takový flash disk, který se pyšnil certifikátem FIPS 140-2, a přesto obsahoval chyby. To nakonec vedlo k obejití ochran a dešifrování obsahu disku. Vzbudilo to značný rozruch, neboť toto se zatím u certifikovaných produktů nestalo. Společnost okamžitě vydala opravu firmware, ovšem vyrobené disky už opravit nešlo. Jak k tomu mohlo dojít? Z procesu odhalení chyby je velmi pravděpodobné (i když ne výslovně uvedené), že chybu obsahoval skutečně certifikovaný firmware. Mohla být také zanesena až ve variantě pro výrobu. Ani jedno z toho se však nesmí stát, verzování je přísně sledované a není možné „upravovat“ certifikovaný firmware, i když v dobré víře. Dobrá víra se zde projevila v tom, že informace o aktuálním heslu uživatele byla zanesena do části disku přístupné zvenčí a sloužila ke kontrole správnosti hesla. Informace pro kontrolu hesla je nutná, avšak nesmí být v žádném případě přístupná zvenčí a kontrola nesmí být udělána přímo tak, jak se na školách učí, že se to právě dělat nesmí. V přístupné části disku byla uložena přímo hodnota haše hesla! Z metod odvozování klíčů z hesel, jak jsme ukazovali v tomto seriálu před nedávnem, víme, že na to jsou za prvé normy NISTu, které byly hrubě opomenuty, a za druhé, že v každém případě se musí použít tzv. sůl. Čili náhodná hodnota, přičleněná k heslu, a poté s ním dohromady zhašovaná. Výsledná haš musí být uložena uvnitř chráněného hardwaru. Náhodná sůl vylučuje použití předem připraveného slovníku hesel a jejich haší, který byl zde skutečně použit k rozlomení. Navíc, proces hašování nesmí mít jednu iteraci (jedno hašování), jako tomu bylo zde, ale milion nebo 10 milionů iterací, jak je doporučováno normou. To značně ztíží až znemožní vytváření

slovníku pro danou konkrétní sůl i útok na jeden konkrétní flash disk. Všechny tyto principy, o nichž jsme psali v předchozích dílech seriálu aplikované kryptologie, byly porušeny. Na druhou stranu, postačila drobná oprava firmware, aby se tento flash disk změnil ve velmi bezpečný datový trezor. Domníváme se, že výjimka potvrzuje pravidlo, takže certifikační odbor NISTu má tuto chybičku, která se vloudí maximálně jednou za dvacet let za sebou a my bychom mohli certifikovaným produktům zase důvěřovat.

Osobní šifrovaný flash disk

V případě, že se nejedná o organizaci, ale o osobní data, která si chceme chránit na svých počítačích doma nebo na pracovišti a nemůžeme stále hlídat, co na disk zapisujeme, je situace odlišná. S flash diskem se ve většině případů nebudeme pohybovat v bezpečném prostředí, protože neuhlídáme všechny počítače, kde budeme flash disk chtít použít a načítat z nich data nebo je tam ukládat, např. na pracovních schůzkách, u přátel, obchodních partnerů apod. Přesto chceme, aby zejména při ztrátě disku nemohl naše privátní nebo obchodní data nikdo získat (třeba data vlastní živnosti, firmy nebo prostě jen osobní data). Zde je několik rizik, které prostě nemůžeme v nebezpečném prostředí odstranit. Zejména se jedná o možnost, že při připojení flash disku k počítači a vložení hesla bude disk otevřen jakémukoliv malwaru z daného počítače. Ten si může na pozadí nějaké úlohy z disku stáhnout naše data nebo tam zanese vir či malware. Horší by ale bylo, kdyby na hostitelském počítači byl klávesnicový čmuchal a naše heslo odchytil a zaznamenal, ať už pro našeho kamaráda, nebo pro někoho jiného. Zatímco první hrozbě lze zabránit ztěží, druhé hrozbě zabránit lze. Heslo lze totiž zadávat zcela mimo připojený osobní počítač, a to přímo na flash disku, pokud je vybaven klávesnicí. Zpočátku se takové šifrované flash disky ani nevyráběly, ale dnes jsou stále častější. Navíc je někdy na flash disku i skener na otisk prstu. Prostřednictvím klávesnice flash disku můžeme tedy zabránit odchycení hesla. Nemůžeme ale zabránit, aby v nebezpečném prostředí byl flash disk „vysát“ nebo poškozen nějakým malwarem. Šifrování on-the-fly malwaru nijak nebrání, neboť v době otevření disku se tento chová zcela transparentně vůči operačnímu systému jako nešifrovaný. Vlastní šifrování a dešifrování provádí až hardware disku pod vrstvou spojení s počítačem. Zajišťuje pouze to, že data budou uložena do flash disku šifrovaná, nijak však data nevyhodnocuje. To znamená, že nebezpečný počítač nám klidně zaviruje i šifrovaný flash disk. Opatření s klávesnicí je ale pro nás velice významné, neboť chrání náš velmi důležitý klíč k flash disku. Nechrání data v době připojení k počítači, to je logické, protože data flash disku mají být právě počítači zpřístupněna. Pokud budeme chtít navíc chránit i data v tomto okamžiku, musíme aplikovat nové opatření. Jistě byste na něj přišli sami. V tomto okamžiku máme zpřístupněn flash disk operačnímu systému. Jak chránit naše data, která si chceme před operačním systémem hostitelského počítače chránit? Opět šifrováním. Postačí je mít zde uložena zašifrovaně klíčem toho, komu patří. Například svoje privátní data můžeme mít uložena v šifrovaném archivu typu winzip, 7zip nebo rar svým klíčem. Ostatní data zde mohou být uložena volně, nešifrovaně nebo šifrovaně klíčem toho, komu mají být předána, nebo otevřeně, pokud na nich tolik nezáleží. Čili na flash disk se musíme dívat jinak při jeho přenášení, jinak při jeho připojení k chráněnému počítači a jinak při připojení k nechráněnému počítači. Pokud aplikujeme uvedená opatření, je riziko útoku na náš flash disk mizivé. Počítač (malware) může sice naše privátní data nahrát z flash disku, ale nic z nich mít nebude, budou šifrována. Klíč k flash disku z nás také nedostane, protože ten zadáváme do hardwaru flash disku na jeho klávesnici. Útok na náš disk by musel být sofistikovanější a dělaný na zakázku. Riziko prolomení našich ochran je však mizivé, a tak lze docílit vysokého stupně ochrany dat. Otázka je, kolik taková ochrana stojí a zda nepoužít softwarové šifrování typu Truecrypt (pokračování příště).

Vlastimil Klíma, kryptolog,
vlastimil.klima@knzsro.cz

LITERATURA

[1] Klíma, V., Rosa, T.: Kryptologie pro praxi (48) – Šifrování USB Flash disků zdarma, Sdělovací technika, 8/2007, str. 9.

[2] Klíma, V., Rosa, T.: Kryptologie pro praxi (47) – Šifrování datových úložišť, Sdělovací technika, 7/2007, str. 18.

[3] Články jsou dostupné elektronicky na osobních stránkách autora.