Výsledky bezpečnostního auditu TrueCryptu

Ing. Josef Kokeš

CryptoFest 2015

Obsah

- TrueCrypt
- Bezpečnostní audity TrueCryptu
- Audit č. 1
- Audit č. 2
- Zhodnocení
- Diskuse

TrueCrypt

- Populární nástroj pro šifrování disků pro Win/Linux/Mac
- Free (as beer), open-source
  - Ale uzavřená skupina vývojářů, neznámí autoři
- Dosud nebyl prolomen
- 2014 autoři podivným způsobem ukončili vývoj
  - Přesto je stále používán
  - Několik odvozených projektů: VeraCrypt, CipherShed

Bezpečnostní audity TrueCryptu

- Cíl: Zjistit, zda je TC bezpečný
- Proč: Důvěřujeme TC, ale nemáme jistotu
  - Způsob ukončení vývoje vzbudil pochybnosti
- Několik dílčích auditů:
  - V. Klíma 2007
  - Ubuntu Privacy Remix 2011
- Open Crypto Audit.org 2013-15 – série auditů:
  1. Kvalita programového kódu
  2. Kryptografická kvalita

Open Crypto Audit Phase 1

- Zahájen 2013, ukončen 2/2014
- Provedl: iSEC Partners
- Zaměření: Kvalita programového kódu
  - TrueCrypt v 7.1a
  - Bootovací kód, instalační program, driver pro Windows
- Neřeší zejména:
  - Kryptografii
  - Šifrování datových kontejnerů
  - Skryté svazky

Výsledky Open Crypto Audit 1

- 11 slabých míst (nejvýše střední závažnost)
  - Málo iterací v algoritmu PBKDF2 (střední)
    - Nedostatečně chrání proti hádání hesel
  - Místy nesprávné testy vstupních dat
  - Místy nesprávná práce s citlivými daty
  - Mnohdy nedodržuje defenzivní přístup k kódu
- Většina slabin není exploitovatelná, pokud uživatel dodrží stanovená doporučení (fyzická bezpečnost, šifrování systému atd.)
  - Jenže většina uživatelů ta doporučení dodržet nedokáže

Open Crypto Audit Phase 2

- Zahájen 2014, dokončen 3/2015
- Provedl: Cryptography Services
- Zaměření: Kryptografie
  - Funkce provádějící šifrování dat
  - Generování klíče z hesla
  - Práce s hlavičkou šifrovaného kontejneru
  - Implementace AES, XTS
- Neřeší zejména:
  - Skryté svazky
  - Ostatní šifrovací algoritmy

Výsledky Open Crypto Audit 2

- Čtyři nalezené slabiny:
  1) Nevhodně ošetřené selhání CryptAcquireContext
  2) Implementace AES náchylná k časovacím útokům
  3) Nesprávná práce s keyfiles
  4) Nevhodně autentizovaný šifrový text v hlavičce kontejneru

Nevhodně ošetřené selhání CryptAcquireContext

- Závažnost: Vysoká
- Složitost provedení útoku: Nezjištěná
- Problém: TrueCrypt ve speciálních případech tiše zahodí případnou chybu a pokračuje se získáváním entropie z jiných zdrojů, považovaných za slabší.
- Důsledek: Náhodnost klíče je menší, než si uživatel myslí.
- Komentář: Závažná chyba, otazník nad přístupem autorů
  - Praktická realizace chyby je složitá
  - Autoři TC možná mají dojem, že entropie z dalších zdrojů je dostatečná
  - Snadná oprava

Implementace AES náchylná k časovacím útokům

- Závažnost: Vysoká
- Složitost provedení útoku: Vysoká
- Problém: Není zajištěno, že dílčí operace AES proběhnou v konstantním čase. Podvrhnutím vlastních dat a měřením doby zpracování může útočník získat informaci o klíči.
- Důsledek: Až odhalení klíče.
- Komentář:
  - Mimořádně obtížné na realizaci, útočník by musel mít přístup, který mu umožní mnohem efektivnější útoky
  - Není jasné, jak přesně by útočník podvrhoval svoje data
  - Obtížné na opravení

Nesprávná práce s keyfiles

- Závažnost: Nízká
- Složitost provedení útoku: Vysoká
- Problém: Z klíčového souboru se čte omezené množství dat. To se navíc do klíče transformuje v podobě CRC, které je velmi slabé. Mnohem slabší řešení než převod hesla na klíč.
- Důsledek: Slabá dodatečná entropie. Útočník může podvrhnout takové soubory, že jejich entropii eliminuje úplně.
- Komentář:
  - Uživatel je opět uváděn v omyl ohledně úrovně bezpečnosti
  - Podvržení souborů je obtížně realizovatelné (a když už je útočník zná, proč by to dělal?)

Neautentizovaný šifrový text v hlavičce kontejneru

- Závažnost: Nezjištěná
- Složitost provedení útoku: Vysoká
- Problém: Slabý algoritmus pro kontrolu integrity hlavičky (CRC, magický řetězec “TRUE”), umožňuje snadné vytváření falešných hlaviček, které TrueCrypt považuje za správné.
- Důsledek: Není jasný. Kryptologicky jde o problém, prakticky spíš ne.
- Komentář:
  - Útočník může nepoznaně změnit hlavičku, ale ne předvídatelným způsobem. Možná DoS?
  - Snadná oprava

Zhodnocení

- TrueCrypt není dokonalý
  - Chyba s CryptAcquireContext je vážný problém pro důvěryhodnost autorů
- Objevené chyby ale nejsou kritické, dají se snadno opravit a obtížně zneužít.
- Rozhodně nejsou důvodem TrueCrypt nepoužívat
  - Zvlášť s ohledem na audity alternativ
- Pozor, nebyl auditován celý kód!

Diskuse

- Máte-li nějaké otázky, teď je na ně vhodná chvíle