Portál pre odborné publikovanie ISSN 1338-0087

Zachytenie šifrovacích kľúčov pomocou analýzy operačnej pamäte a čitateľné heslá v pamäti II.

Pondelík Matej · Informačné technológie, Študentské práce

05.11.2010

V predchádzajúcej časti článku sme si spravili úvod do šifrovania a popísali metódy na zachytenie šifrovaných hesiel použitých šifrou AES z operačnej pamäte, ako aj ich získať rôznymi technikami. Predstavili sme si aj open-source softvér TrueCrypt na šifrovanie dát v reálnom čase. V tejto časti si ukážeme názorné ukážky zachytenia šifrovacích kľúčov v operačných systémoch Ubuntu a Windows.

4. Zachytenie šifrovacích kľúčov v Ubuntu

V časti 3.1. sme si ukázali ako získať výpis obsahu pamäte konkrétneho procesu. Navyše si môžeme vybrať, ktorý sektor pamäte chceme vypísať, prípadne ak poznáme presnú adresu hesla v pamäti, vypísať len heslo. Teraz sa zameriame na hľadanie šifrovacích hesiel, ktoré používa TrueCrypt pri šifrovaní algoritmom AES. Príklad uvedieme na počítači so 64-bitovým operačným systémom Ubuntu 9.10.

Ak máme fyzický prístup k počítaču, na ktorom je za pomoci TrueCryptu pripojený šifrovaný disk a máme rootovské práva môžeme pomocou analýzy pamäte získať šifrovacie heslá. Treba upozorniť, že užívateľské heslo, ktoré slúži na odvodenie šifrovacích hesiel sa vo výpise pamäti nenachádzalo. V tomto prípade sú hľadané šifrovacie heslá nasledovné:

- primárny kľúč: f306 f742 b16e 9195 267a 23c2 1974 0a43 c669 201e c049 7ad5 4bce 50e2 0ac6 65ff
- sekundárny kľúč: 3728 a4fb 77c4 191f 476c 0775 2168 f6ba a905 75a9 c420 f9e4 f112 ad2e f10a 38b8

Analýzou rôznych výpisov pamäte sme zistili, že šifrovacie heslá sa nachádzajú v halde posledného procesu, ktorý TrueCrypt vytvoril. Toto nám znížilo požiadavky na čas získania výpisu, zachytenie hesiel a veľkosť výpisu z niekoľkých GB (v prípade výpisu obsahu celej pamäte) len na približne 1 MB. Takýto skrátený výpis, v ktorom sú zvýraznené heslá je uvedený nižšie (tab. 1). Podľa našich zistení sa ukázalo, že hlavný kľúč sa v halde nachádza trikrát a sekundárny kľúč štyrikrát.

Tab. 1. Výpis haldy

offset	

0058330	0550 0000 0000 0000 0110 0000 0000 0000
0058340	f306 f742 b16e 9195 267a 23c2 1974 0a43
0058350	c669 201e c049 7ad5 4bce 50e2 0ac6 65ff
0058360	3728 a4fb 77c4 191f 476c 0775 2168 f6ba
0058370	a905 75a9 c420 f9e4 f112 ad2e f10a 38b8
0058380	0000 0000 0000 0000 0000 0000 0000 0000
…	…
0058440	0000 0000 0000 0000 01f1 0000 0000 0000
0058450	f306 f742 b16e 9195 267a 23c2 1974 0a43
0058460	c669 201e c049 7ad5 4bce 50e2 0ac6 65ff
0058470	e560 430f 540e d29a 7274 f158 6b00 fb1b
…	…
0058620	8c71 4fe4 f306 f742 b16e 9195 267a 23c2
0058630	1974 0a43 00e0 0000 01f1 0000 0000 0000
0058640	3728 a4fb 77c4 191f 476c 0775 2168 f6ba
0058650	a905 75a9 c420 f9e4 f112 ad2e f10a 38b8
0058660	5b88 c3fc 2c4c dae3 6b20 dd96 4a48 2b2c
…	…
0058810	e497 dbd3 3728 a4fb 77c4 191f 476c 0775
0058820	2168 f6ba 00e0 0000 b751 0001 0000 0000
0058830	0000 0000 0000 0000 0000 0000 0000 0000

Fakt 1

Z týchto výskytov kľúčov bude pre nás zaujímavá najmä zvýraznená oblasť, kde oba šifrovacie kľúče nasledujú za sebou (s posunutím od začiatku súboru o 58180_{16}). Na počítači so 64 bitovým systémom a s 2 GB RAM sa tieto heslá nachádzali vždy približne na rovnakej pozícii. Najmenší posun od začiatku súboru, ktorý bol zatiaľ zaznamenaný je 58140_{16}. Z ďalších zistení sme odvodili vzťah na približné určenie pozície týchto hesiel: $58140_{16} \pm 10_{16} * x_{16}$, kde x je malé číslo, ktoré budeme postupne zväčšovať od nuly (v šestnástkovej sústave – 0, 1,...A,...). Výsledné pozície budú napríklad x_{16} 58140_{16}, 58150_{16}, 58160_{16}, atď.

Fakt 2

Ďalšia možnosť ako identifikovať túto oblasť, kde sú uvedené oba kľúče je, ak si všimneme hrubým písmom zvýraznené posuny vo výpise. Vzdialenosť hlavného kľúča vo zvýraznenej oblasti od jeho ďalšieho výskytu je pre 64 bitový systém 00058450_{16} – 00058340_{16} = 110_{16} (272) bajtov a pre 32 bitový systém 108_{16} (264) bajtov. Tieto posuny boli počas všetkých testov rovnaké.

Ak vezmeme do úvahy druhý spomínaný fakt, nájdenie kľúčov by mohlo spočívať v porovnávaní 256 bitových reťazcov s reťazcami, ktoré sú od týchto reťazcov vzdialené o 110_{16} bitov (pre 64-bit systém). V prípadne zhody sme s vysokou pravdepodobnosťou našli oblasť, v ktorej sa nachádza hlavný aj sekundárny šifrovací kľúč. V prípade, že

zvážime aj fakt číslo 1, budeme porovnávať najprv reťazce, ktoré sa nachádzajú v súbore s posunom 58140_{16} $\pm 10_{16}$*x_{16}.

Fakt 3

Neskorším skúmaním sme prišli na to, že oblasti, ktoré sa v hore uvedenom výpise vyskytujú s posunom:

- 58450 až 58633 – na začiatku oblasti sa nachádza primárny kľúč a na jej konci sa nachádza prvá polovica primárneho kľúča,
- 58640 až 58823 – na začiatku oblasti sa nachádza sekundárny kľúč a na jej konci sa nachádza prvá polovica sekundárneho kľúča.

Tieto oblasti dát sa nachádzajú aj vo výpise operačnej pamäti Windowsu a majú veľkosť 484 bajtov. Z tohto môžeme vyvodiť ďalšie podmienky na lokalizáciu šifrovacích kľúčov. Navyše celá oblasť, sa nachádza vo výpise haldy ako prvá súvislá oblasť dát od konca súboru, takže sa dá nájsť pomerne jednoducho aj prezeraním výpisu v hexadecimálnom editore. Okrem šifrovacích hesiel sa v tomto výpise ešte nachádzajú ďalšie informácie o šifrovanom zväzku, a to:

- použitá šifra,
- šifrovací mód,
- veľkosť bloku dát,
- veľkosť kľúča,
- použitá verzia TrueCryptu
- ktorá partícia prípadne súbor sa šifruje.

5. Zachytenie šifrovacích hesiel vo Windowse

Momentálne nevieme určiť, kde presne hľadať šifrovacie kľúče ako v prípade Ubuntu, no dajú sa lokalizovať vo výpise operačnej pamäti, podľa nasledujúcich pravidiel, ako je aj vidieť vo výpise nižšie (tab. 2):

- prvých 64 bajtov šifrovaného zväzku vytvoreného TrueCrypt-om tvorí salt [8]. Tento salt, ktorý získame zo zašifrovaného disku vyhľadáme vo výpise pamäti,
- s posunom -256 bajtov od saltu sa nachádza sekundárny kľúč,
- s posunom -512 bajtov od saltu sa nachádza primárny kľúč, za ktorým hneď nasleduje sekundárny kľúč (zvýraznená oblasť).

Tab. 2 Oblasť so šifrovacími heslami z Windowsu

offset	
0000000	f306 f742 b16e 9195 267a 23c2 1974 0a43
0000010	c669 201e c049 7ad5 4bce 50e2 0ac6 65ff
0000030	3728 a4fb 77c4 191f 476c 0775 2168 f6ba
0000040	a905 75a9 c420 f9e4 f112 ad2e f10a 38b8
0000050	0000 0000 0000 0000 0000 0000 0000 0000
…	…

0000100	3728 a4fb 77c4 191f 476c 0775 2168 f6ba
0000110	a905 75a9 c420 f9e4 f112 ad2e f10a 38b8
0000120	0000 0000 0000 0000 0000 0000 0000 0000
…	…
0000200	d336 3ac3 0295 a4d0 3ef6 d1b2 6aa4 58e3
0000210	b11a 2f2e d0e4 854f c32a b3a3 4860 9226
0000220	b024 2ac0 35a8 1944 08cb 456a 9925 ced8
0000230	6b07 362c 6892 7a85 4c12 2978 52af 6f91

6. Použitie získaných šifrovacích hesiel

Ak sme získali šifrovacie kľúče a máme prístup ku šifrovanému zväzku, na jeho dešifrovanie budeme musieť tento zväzok trochu "orezať". TrueCrypt na začiatok každého šifrovaného zväzku vytvára dve hlavičky. Jedna hlavička slúži na pripojenie klasického šifrovaného zväzku a druhá pre prípadný skrytý zväzok. V prípade, ak sa na šifrovanom zväzku nenachádza skrytý zväzok, je oblasť určená pre jeho hlavičku vyplnená náhodnými dátami. Každá z týchto hlavičiek má veľkosť 65536 bajtov. Zároveň sa na konci šifrovaného zväzku nachádzajú zálohy týchto hlavičiek s rovnakou veľkosťou [8]. Čiže, ak chceme dešifrovať zväzok vytvorený pomocou TrueCrypt-u musíme odstrániť prvých a posledných 131072 bajtov tohto zväzku. Vzniknutý súbor potom môžeme dešifrovať za pomoci získaných kľúčov.

7. Passware Password Recovery Kit Forensic

Tento komerčný softvér okrem iného dokáže v najnovšej verzii dešifrovať zväzky šifrované pomocou TrueCrypt-u alebo BitLocker-u, no je použiteľný len pod Windowsom. V demo verzii je schopný zo súboru ktorý obsahuje výpis operačnej pamäte počítača, na ktorom je pripojený šifrovaný zväzok, získať šifrovacie heslá používané TrueCrypt-om a následne tento zväzok dešifrovať (v demo verzii len do veľkosti 64 MB). V platenej verzii ($795) umožňuje získanie obrazu operačnej pamäti z druhého počítača pomocou firewire.

Šifrovacie heslá hľadá zrejme tou istou metódou aká je spomínaná v tomto dokumente v časti 5. Ak mu zadáme vstupný súbor s totožnou štrukútov ako je súbor zobrazený v tabulke 2, dešifrovanie prebehne úspešne. Ak pozmeníme posuny kľúčov, dešifrovanie zlyhá pretože program nebol schopný nájsť šifrovacie kľúče. Z toho vyplíva že ak poznáme šifrovacie kľúče a máme k dispozícii zašifrovaný zväzok môžme ho dešifrovať použitím tohto programu tak, že miesto obrazu celej pamäte použijeme súbor, ktorý si vytvoríme podľa pravidiel uvedených v časti 5.

8. Vyhľadávanie iných hesiel

Pri našom výskume sme sa v skratke zamerali aj na vyhľadávanie užívateľských hesiel alebo rôznych prístupových hesiel. Uveďme, že nezahešované heslá v textovej podobe boli detekované v halde (podobne ako pri TrueCrypte) vlastného procesu. Takto boli nájdené prístupové heslá do zaheslovaných archívov .rar a .zip, do zaheslovaných dokumentov pdf alebo prístupové heslo k účtu icq cez klient Pidgin.

8.1. Vyhľadanie prístupového hesla do archívu .rar

Po otvorení zaheslovaného súboru archív.rar a zadaní hesla sa vytvorí noví proces: file-roller. Spomínaným spôsobom urobíme výpis haldy tohto procesu

Tab. 3. Heslo v halde procesu file-roller.

8701 0000 0000 0000 9a00 0000 0000 0000	|.....|
4d65 7461 0000 0000 2100 0000 0000 0000	|Meta....!.....|
2d70 6865 736c 6f72 6172 3132 3300 0000	|-pheslorar123.....|
2000 0000 0000 0000 5100 0000 0000 0000	| .....Q.....|

Heslo sa vo výpise nachádza štyri krát, z toho minimálne raz ho uvádza reťazec -p, pred ktorým sa nachádzajú minimálne tri nulové znaky.

8.2 Keyring – Proces:gnome-keyring-d

Tentokrát pre nás nebude zaujímavý výpis haldy, ale adresa, ktorá je približnie na riadku 137 v súbore /proc/[pid]/maps. Dôležité je aby sa nachádzala za adresou, ku ktorej pristupuje súbor /usr/.../LC_MESSAGES/gnome-keyring.mo alebo usr/.../LC_MESSAGES/libc.mo (tab. 4).

Tab. 4. riadky 135 – 137 súboru /proc/[pid]/maps

135	7fcee4f40000-7fcee4f41000 r–p 00000000 08:05 129230
	/usr/share/locale-langpack/sk/LC_MESSAGES/libc.mo
136	7fcee4f41000-7fcee4f44000 r–p 00000000 08:05 129406
	/usr/share/locale-langpack/sk/LC_MESSAGES/gnome-keyring.mo
137	7fcee4f44000-7fcee4f48000 rw-p 00000000 00:00 0
138	7fcee4f48000-7fcee4f4a000 rw-p 00000000 00:00 0

Tab. 5. Výpis obsahu zvýrazneného pamäťového miesta

Offset	Plaintext
00000000	|........login123|
...	...
00000120	|.....|
00000130	|........icqpsswd|
00000140	|.....|
00000150	|........email123|

Ako prvé sa tu nachádza užívateľské prístupové heslo do systému, v prípade operačného systému Ubuntu sa dá použiť na prístup k rootovským právam. Ďalej sa tu nachádza heslo pre internetový komunikátor Pidgin, a ako posledné prístupové heslo k emailovému klientovi Evolution, ktorý bol zo systému odstránený pred niekoľkými mesiacmi. Pritom ako jediné heslo, ktoré malo byť systémom používané bolo heslo pre

komunikátor Pidgin aby bolo možné automatické prihlasovanie.

Podľa nás je to spôsobené aplikáciou Seahorse (Passwords and Encryption Keys), ktorá si zapamätá každé novo vložené heslo. Takže len po nainštalovaní systému a prihlásení sa, môžeme nájsť prihlasovacie heslo v procese gnome-keyring-d. Po prvom prihlásení, napríklad ku účtu icq, bude gnome-keyring-d obsahovať už aj toto heslo. Po odstránení položky hesiel z aplikácie Seahorse, neboli už tieto heslá uložené v pamäti procesu gnome-keyring-d. Treba uviesť, že tieto heslá boli lokalizované len v 64-bitovom systéme.

9. Zhodnotenie

Na záver môžme povedať, že TrueCrypt je kvalitný nástroj na šifrovanie dát, ale aj keby boli dáta šifrované nezlomitelnou šifrou, bolo by to zbytočné, pretože existuje iná cesta ako získať šifrovacie heslá. Toto neplatí len pre TrueCrypt ale pre všetky šifrovacie programy. Pomocou popísaných techník, prípadne ich kombináciou sme schopný nájsť šifrovacie kľúče aj šifrované zväzky v systéme.

Odkazy na literatúru

1. TrueCrypt, “TrueCrypt Home Page,” 2010; http://www.truecrypt.org/docs/
2. Dworkin, M., Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, NIST Special Publication 800-3E, January 2010, Dostupné na internete: http://csrc.nist.gov/publications/nistpubs/800-38E/nist-sp-800-38E.pdf
3. Dornseif, M., “0wned by an iPod” Laboratory for Dependable Distributed Systems, PacSec 2004, Dostupné na internete: http://md.hudora.de/presentations/firewire/PacSec2004.pdf
4. Boileau, A., “Hit By A Bus: Physical Access Attacks with Firewire” Security-Assessment.com, Ruxcon 2006, Dostupné na internete: http://www.storm.net.nz/static/files/ab_firewire_rux2k6-final.pdf
5. Alex, J.H., Schoen, S.D., Heninger, N., Clarkson, W., Paul, W., Calandrino, J.A., Feldman, A.J., Appelbaum, J., Felten, E.W., Last we remember: cold-boot attacks on encryption keys. February 2008, Dostupné na internete: http://citp.princeton.edu/pub/coldboot.pdf
6. The Center for Information Technology Policy, Princeton University, http://citp.princeton.edu/memory/code/
7. wikihow, “wikihow Home Page,” 2010; http://www.wikihow.com/Force-a-Blue-Screen-in-Windows
8. TrueCrypt, “TrueCrypt Documentation,” 2010; http://www.truecrypt.org/docs/
9. Pasware, Inc., “Passware Kit Forensic 9.7,” 2010; http://www.lostpassword.com/kit-forensic.htm

---

Spoluautorom článku je Ing. Štefan Balogh, Fakulta elektrotechniky a informatiky,Katedra aplikovanej informatiky a výpočtovej techniky, Slovenská technická univerzita