Dyski samoszyfrujące. Czy są alternatywą dla dm-crypta?

Kamil Breczko

kamil.breczko@gmail.com

1 Czym jest szyfrowanie i dlaczego szyfrować?

Szyfrowanie dysku jest to technologia, która pozwala na utajnieniu danych umieszczonych na dysku, szyfrując każdy bajt danych. Z pomocą szyfrowania użytkownik komputera jest w stanie utrudnić kradzież tajnych danych. Przydaje się przede wszystkim wtedy, kiedy urządzenie narażone jest na kradzież lub odczytanie danych umieszczonych w pamięci urządzenia przez osoby nieuprawnione. Szyfrowanie zalecane jest nie tylko dla osób, które przechowują zastrzeżone dane firm czy pacjentów, ale także użytkownikom prywatnym w celu zabezpieczenia się przed odczytaniem danych po sprzedaży czy też po utracie dysku. Szyfrowanie danych może odbywać się z poziomu systemu plików oraz na poziomie sektorowym. Szyfrowanie na poziomie sektorowym w porównaniu do szyfrowania na poziomie plików pozwala na zabezpieczenie większość danych, które znajdują się na dysku. Istnieje wiele różnych metod do szyfrowania danych na dysku. Należą do nich oprogramowania przeznaczone do tego celu oraz rozwiązania sprzętowe. W tym artykule poznamy jak działają tego typu metody oraz odpowiemy sobie na pytanie, czy podane metody skutecznie chronią naszą prywatność oraz czy dyski samoszyfrujące w pełni mogą zastąpić szyfrowanie programowe.

2 Jak działa szyfrowanie programowe?

Na rynku istnieje wiele oprogramowań płatnych jak i darmowych do szyfrowania dysków programowo. Za przykład posłuży nam dm-crypt, który jest otwartym oprogramowaniem, umożliwiającym szyfrowanie całych partycji w czasie rzeczywistym. Oprogramowanie dm-crypt działa na poziomie jądra w warstwie między systemem plików a sprzętem. Charakteryzuje się szyfrowaniem blokowym, który przyjmuje na wejściu blok o określonej długości oraz klucz szyfrujący, a zwraca blok zaszyfrowany o tej samej długości.

Używając oprogramowania dm-crypt w połączeniu z systemem LUKS (Linux Unified Key Setup) do zarządzania hasłami, wprowadzamy większe możliwości dla szyfrowania dysku. Z pomocą LUKS nie potrzebujemy zapamiętywać klucza do szyfrowania dysku, którego nie można zmienić w przypadku ujawnienia. Dlatego użytkownik ma możliwość do posiadania 8 haseł, które odwzorowywane są na klucz szyfrujący. Podawane hasła są ustalane przez użytkownika z możliwością zmiany. Aby taka możliwość była dostępna, LUKS przechowuje metadane na początku partycji w postaci niezaszyfrowanej. Informacje o kluczach, które będą generowane przez funkcje PBKDF2 na podstawie hasła użytkownika są zapisywany w tak zwanych slotach. W każdym slocie znajduje się zaszyfrowana kopia klucza głównego oraz parametry potrzebne dla

Instytut Informatyki Uniwersytetu Wrocławskiego, 2017–2018
Esej przygotowany w ramach zajęć *Kultura bezpieczeństwa komputerowego*

funkcji PBKDF2: liczba iteracji mieszania oraz sól. Użyte parametry w funkcji PBKDF2 zwiększają entropie hasła, chroniąc przed atakami słownikowymi oraz tęczowymi tablicami. Atak za pomocą tęczowych tablic polega na dopasowaniu pary hash-hasło do wcześniej wykradzionego hasza. [**?**]

Po wprowadzeniu w system hasła użytkownika, oprogramowanie LUKS korzystając z funkcji PBKDF2 generuje dla każdego slotu po kolei klucz o stałej długości, który służy do odszyfrowania kopii klucza szyfrującego dysk. Jeśli klucz szyfrujący będzie poprawny to umieszczany jest w pamięci RAM, w celu szyfrowania i deszyfrowania bloków pamięci. W nagłówku LUKS można znaleźć takie informacje jak:

- wersja LUKS;
- algorytm szyfrowania np. AES;
- tryb szyfrowania np. cbc-essiv: sha256;
- suma kontrolna klucza głównego;
- rozmiar klucza głównego;
- UUID;

Co się stanie jeśli nagłówek zostanie uszkodzony? W tym przypadku nie jesteśmy w stanie odszyfrować urządzenia, dlatego zalecana jest metoda odłączenia nagłówka lub zrobienia kopii na innym dysku. W przypadku odłączenia nagłówka na dysku widoczne są tylko zaszyfrowane dane, bez ujawnienia sposobu szyfrowania. [**?**]

W celu zmaksymalizowania bezpieczeństwa używa się dm-crypt z ustawionym szyfrem symetrycznym AES oraz trybem zapisu XTS. Aktualnie, uważa się że *"tryb XTS to jeden z najnowszych trybów szyfrowania, który zapewnia lepszą ochronę niż tryby CBC i ECB "*. Do przekształcenia bloków używa dwukrotnie klucza AES. Pierwszy z nich służy do szyfrowania blokowego AES, a drugi do wartości modyfikującej, na którym działa funkcja logiczna XOR oraz funkcja wielomianowa Galois. Powyższa metoda szyfrująca podwójnie dane, zapewnia że z dwóch identycznych bloków otrzymamy dwa różne zaszyfrowane bloki. [**?**]

3 Jak działa szyfrowanie sprzętowe - dyski samoszyfrujące?

Samoszyfrujące dyski twarde, zwane SED (self-encrypting hard drive), automatycznie szyfrują wszystkie dane w czasie rzeczywistym, które znajdują sie na nośnikach. Oznacza to, że przy każdym dostępie do pliku, dane są szyfrowane i odszyfrowywane. Zabezpieczanie danych jest całkowicie niewidoczne dla użytkownika, co powoduje że użytkownik nie musi samodzielnie zabezpieczać danych. Wszystkim zajmuje się kontroler dysku.

Używając dysków SED, szyfrowaniem i deszyfrowaniem danych na dysku zajmuje sie dedykowany procesor, który jest zintegrowany z dyskiem. Większość producentów dysków SED dostarcza także wsparcie szyfru AES dla procesora. Takie rozwiązanie tworzy znaczną przewagę nad rozwiązaniem programowym, w którym za szyfrowaniem i odszyfrowaniem odpowiada procesor komputera. Po wyprodukowaniu dysku SED, każdy nośnik posiada w pamięci fabrycznie losowo wygenerowany klucz szyfrujący, który ma pomóc chronić nasz dysk, szyfrując i rozszyfrowując dane. Tym samym domyślnie jest włączone szyfrowanie danych na dysku. Więc, w jaki sposób kontroler dysku zna klucz główny? W przypadku nowego dysku, klucz główny jest przechowywany w formie zwykłego tekstu, dopóki użytkownik nie zdecyduje się na tryb z uwierzytelnieniem. Po tej operacji, podobnie jak w szyfrowaniu programowym, dysk udostępnia dwupoziomowe szyfrowanie. Klucz główny zostaje zaszyfrowany kluczem uwierzytelnienia, który powstaje z hasła wpisanego przez użytkownika. W celu weryfikacji hasła, dysk przechowuje w postaci jawnej haszowany klucz uwierzytelnienia. W przypadku gdy klucz uwierzytelnienia nie

jest zgodny zawartośc dysku pozostaje ukryta przed użytkownikiem. System udostępnia widok tylko na te dane, które są potrzebne do wyświetlenia interfejsu dla użytkownika, w celu wprowadzenia hasła. Po poprawnym zweryfikowaniu klucza użytkownika, system umożliwiwa wgląd na rzeczywisty rozmiar dysku. Dyski SED przechowują klucze szyfrujące wewnątrz napędu, wykonując całą kryptografię w sterowniku dysku, tym samym zmniejszając ryzyko przechwycenia kluczy przez hakerów z pamięci RAM oraz poprawiając wydajność procesora. W celu zwiększenia bezpieczeństwa zaleca się zresetowanie klucza szyfrującego po włączeniu trybu z uwierzytelnieniem. [**?**]

Seagate, producent dysków samoszyfrujących zapewnia dodatkowo szybkie niszczenie danych przy użyciu metody wymazywania kryptograficznego, które polega na zastąpieniu klucza szyfrowania wewnątrz dysku. [**?**]

4 Wady pełnego szyfrowania

Kiedy celem jest bezpieczeństwo prywatnych danych, należy przeanalizować nie tylko zalety, a także wady zastosowania danych technik.

W przypadku szyfrowania programowego większość metod pełnego szyfrowania dysku jest podatna na atak zimnego rozruchu, który polega na kradzieży kluczy szyfrowania z działającego już systemu operacyjnego. Atakujący z fizycznym dostępem do komputera wykonuje twardy reset systemu, a następnie podłącza do niego urządzenie z własnym systemem operacyjnym co pozwoli na przechwycenie danych, które są umieszczone w pamięci RAM, w tym klucze szyfrujące, które umieszczone są w postaci jawnej. Istnieje też możliwość przeniesienia pamięci RAM do innego komputera, bez utraty danych. Wystarczy schłodzić odpowiednio układy pamięci. [**?**] Pojawia się kolejny problem, przy szyfrowaniu programowym, kiedy sektory z systemem operacyjnym muszą zostać odszyfrowane przed uruchomieniem interfejsu z panelem do wprowadzenia klucza użytkownika. W tym przypadku dysk jest narażony na atak złośliwego oprogramowania zwanego bootkit. Bootkit atakuje sektor rozruchowy, modyfikując proces rozruchu i umożliwiając podsłuchanie hasła do dysku. W celu zabezpieczenia się przed atakami, stosuje się dodatkowe warstwy ochrony, takie jak uwierzytelnienie wstępne, ładując mały i zabezpieczony system operacyjny czy też użycie modułu zaufanej platformy (TPM - Trusted Platform Module), który służy do sprawdzenia integralności środowiska rozruchowego. [**?**]

Nie tylko szyfrowanie programowe posiada wady. Pomimo że procesy zabezpieczające w dyskach samoszyfrujących są słabo udokumentowane, znaleziono podatności w poszczególnych typach dysków. Do testów dysków samoszyfrujących użyto dysków Western Digital z serii My-Passport oraz MyBook. Z wyników testów okazało się, że dyski samoszyfrujące mogą słabiej zabezpieczać niż szyfrowanie programowe. Według Matthew Green, asystenta na uczelni uniwersytu Johnsa Hopkinsa, największym problemem w dyskach samoszyfrujących jest generator liczb losowych, ponieważ *" robi to za pomocą funkcji C rand(), która nie jest bezpieczna kryptograficznie "*. Stwierdzono także, że generator liczb losowych przy restarcie klucza szyfrującego wykorzystuje informacje o aktualnym czasie z komputera, a w przypadku klucza fabrycznego użyto daty produkcji dysku. *" Oznacza to, że atakujący może odgadnąć klucz w krótkim czasie za pomocą jednego komputera "*, uważa Green. Kolejnym problemem znajdującym się w dyskach samoszyfrujących jest brak kompatybilności z systemem Linux. Aktualnie dyski samoszyfrujące są kompatybilne z systemem Windows oraz macOS, a użytkownicy systemów Linux są zmuszeni do korzystania z zewnętrznego oprogramowania. Większym problemem jaki ujawniono jest backdoor, który znajduje się w ukrytym sektorze na dysku. Złośliwe oprogramowanie umożliwia przejęcie klucza szyfrującego bez znajomości hasła użytkownika. [**?**] [**?**]

Szyfrowanie programowe oraz za pomocą dysków szyfrujących mają także wspólne podatności. Jedna jak i druga metoda narażona jest na ryzyko utraty danych, w przypadku kradzieży komputera podczas trybu uśpienia lub działającego systemu, ponieważ zaraz po sekwencji rozruchu BIOSu, klucze są odszyfrowywane i używane aż do ponownego rozruchu. W tym przypadku

atakujący bez dużego wysiłku jest w stanie wykraść wszystkie dane, nawet nie znając klucza szyfrującego. W przypadku dysków samoszyfrujących, gdzie klucz znajduje się na dysku, istnieje możliwość kradzieży samego dysku zachowując *" sesje "* z możliwością odczytania każdego pliku. Przykładem jest atak zwany *" hot plug "*, który polega na podłączeniu zewnętrzego źródła zasilania do dysku, po czym zamianie kabli SATA, podłączając dysk do innego komputera. W ten sposób dysk pozostaje odszyfrowany i pod kontrolą hakera. Innym sposobem odczytu danych z dysku samoszyfrującego jest zasymulowanie krytycznego błędu BSOD w systemach Windows, który jest miękkim resetem i dysk po takiej czynności jest dalej odszyfrowany. W trakcie tej czynności haker jest wstanie zmienić źródło rozruchu i uruchomić swój własny system, skąd będzie miał dostęp do całego dysku SED.

Najskuteczniejszym sposobem przed podanymi atakami jest wyłączenie komputera albo wprowadzenie w stan hibernacji, po którym urządzenie zapomina klucz szyfrujący. Dodatkowym sposobem zwiększenia bezpieczeństwa poszczególnych plików jest użycie szyfrowania na poziomie plików. [**?**]

5 Wniosek

Żadna technologia szyfrowania danych nie zapewnia skutecznej ochrony przed wszystkimi istniejącymi zagrożeniami. Atakujący wykorzystują coraz to nowsze techniki i metody do kradzieży danych, dlatego użytkownicy nie powinni się ograniczać do jednej metody zabezpieczania dysku przed osobami nieuprawnionymi do przeglądania tajnych danych. Warto się też zastanowić czy wybierając dysk samoszyfrujący ufamy firmie, która go zaprojektowała. W szyfrowaniu programowo kod, który odpowiada za szyfrowanie/deszyfrowanie jest jawny i każdy może go zweryfikować oraz kontrolować. Łatwo jest różwnież zaktualizować, jeśli problem zostanie znaleziony. Nikt by się nie odważył na wprowadzenie złego oprogramowania, wiedząc że kod jest analizowany przez ludzi, którzy bardzo dobrze znają się na kryptografii. Także zaletą szyfrowania programowego jest większa kontrola użytkownika oraz wybór metod i trybów szyfrowania. Z drugiej strony dyski samoszyfrujące to blackbox. Nie wiemy co dokładnie znajduje się wewnątrz. Według agencji NSA, dyski samoszyfrujące doskonale nadają się do zabezpieczania danych i zawarta w nich technologia nie osłabia zabezpieczeń. Zdaniem NSA *" strażnicy powinni znajdować się jak najbliżej chronionego obiektu "*. Istnieje także możliwość że służby rządowe popierają szyfrowanie danych przez dyski SED, ponieważ porozumieli się z producentami i kontrolują szyfrowanie danych.

Literatura

[1] Adam Golański, *Szyfrowanie całego dysku: ochroń swoje dane przed wścibskimi*, url: `https://www.dobreprogramy.pl/Szyfrowanie-calego-dysku-ochron-swoje-dane-przed-wscibskimi,News,70768.html` (term. wiz. 22. 12. 2017)

[2] Logan, *Encrypted external drive with LUKS*, url: `https://www.loganmarchione.com/2015/05/encrypted-external-drive-with-luks/` (term. wiz. 02. 01. 2017)

[3] Kingston Technology, *Pamięci szyfrowane*, url: `https://www.kingston.com/pl/usb/encrypted_security/xts_encryption` (term. wiz. 20. 12. 2017)

[4] Warwick Ashford, *Self-encrypting drives: SED the best-kept secret in hard drive encryption security*, url: `http://www.computerweekly.com/feature/Self-encrypting-drives-SED-the-best-kept-secret-in-hard-drive-encryption-security` (term. wiz. 22. 12. 2017)

[5] Seagate Technology, *Dyski samoszyfrujące do serwerów i macierzy dyskowych NAS i SAN*, url: `https://www.seagate.com/files/docs/pdf/pl-PL/whitepaper/self-encrypting-drives-tp600.1-0903pl.pdf` (term. wiz. 22. 12. 2017)

[6] Mariusz Błoński, *Cold-boot attack: szyfrowanie nie chroni*, url: `http://kopalniawiedzy.pl/cold-boot-attack-pamiec-RAM-dysk-twardy-szyfrowanie-klucze-kryptograficzne,5371` (term. wiz. 22. 12. 2017)

[7] Uli Ries, *Bootkit bypasses hard disk encryption*, url: `http://www.h-online.com/security/news/item/Bootkit-bypasses-hard-disk-encryption-742721.html` (term. wiz. 22. 12. 2017)

[8] Joseph Cox, *Some Popular 'Self Encrypting' Hard Drives Have Really Bad Encryption*, url: `https://motherboard.vice.com/en_us/article/mgbmma/some-popular-self-encrypting-hard-drives-have-really-bad-encryption` (term. wiz. 22. 12. 2017)

[9] Gunnar Alendal, Christian Kison, modg *On the (in)security of a Self-Encrypting Drive series*, url: `https://eprint.iacr.org/2015/1002.pdf` (term. wiz. 22. 12. 2017)

[10] Lucian Constantin, *Self-encrypting drives are hardly any better than software-based encryption*, url: `https://www.pcworld.com/article/3004670/business-security/self-encrypting-drives-are-hardly-any-better-than-software-based-encryption.html` (term. wiz. 22. 12. 2017)