IT4Sec Reports 113
http://dx.doi.org/10.11610/it4sec.0111

Сигурност на дисковете с пълно хардуерно криптиране. Видове атаки

Веселин Монев

Институт по информационни и комуникационни технологии – БАН
секция “Информационни технологии в сигурността”
www.IT4Sec.org

София, юни 2014 г.

Веселин Монев, Сигурност на дисковете с пълно хардуерно криптиране. Видове атаки**,** *IT4Sec Reports* 113 (София, Институт по информационни и комуникационни технологии, юни 2014 г.), http://dx.doi.org/10.11610/it4sec.0113.

IT4SecReports 113 „Сигурност на дисковете с пълно хардуерно криптиране. Видове атаки“ Пълното хардуерно криптиране на SSD дискове се счита за бърза и сигурна алтернатива на софтуерно-базираните решения като TrueCrypt и Bitlocker. Тъй като ключовете за криптиране се съхраняват вътре в криптиран чип на самия диск или на криптиран дял, вместо в RAM паметта или паметта на главния процесор, традиционните атаки като cold reboot („студент старт“) изглеждат безсмислени. Настоящата работа ще покаже, че в зависимост от конфигурацията пълното хардуерно криптиране на дискове може да е толкова несигурно, колкото е и софтуерното. Причината за това е една удивително проста атака, която експлоатира факта, че самокриптиращия се диск не забелязва дали SATA кабелът е свързан към друг компютър, което ефективно превръща самокриптиращия се диск в самодекриптиращ се такъв.
Разглеждат се още известни атаки от областта на софтуерно-базираните криптозащити и тяхната адаптация в различни компютърни системи, включително лаптопи и настолни конфигурации.

Ключови думи: Пълно дисково криптиране, атаки, DMA, cold boot, hot plug, RAM, SSD, самокриптиращ, сигурност, противодействие, BIOS, защита, техники

IT4Sec Reports 113 “Security of SSD Drives with Full Disk Encryption and Some Attacks “Full disk encryption of SSD drives is considered to be fast and safe alternative to software-based solutions like TrueCrypt and Bitlocker. Since encryption keys are stored in encrypted chip on the disc or on encrypted partition instead of the RAM or the memory of the main processor, the traditional attacks like cold reboot seem not to be applicable. This report demonstrates that, depending on the configuration, full disk encryption can be as uncertain as the software disk encryption. The reason for this is an amazingly simple attack that exploits the fact that the self-encrypting disk does not detect whether the SATA cable is connected to another computer, which effectively turns the self-encrypting disc in self-decrypting one.
Further, the report examines some attacks in the field of software-based disk encryption and their adaptation to different computer systems, including laptops and desktops.

Keywords: Full disk encryption, FDE, attack, DMA, cold boot, hot plug, RAM, SSD, self-encrypting, security, securing, BIOS, protection, techniques, countermeasures

Веселин Монев е студент в магистърска програма „Киберсигурност“ на Нов български университет, София. Работи като „ИТ Инженер“ за Хюлет Пакард в областта на корпоративните сторидж продукти.

ISSN 1314-5614

СЪДЪРЖАНИЕ

Често използвани съкращения 4

ВЪВЕДЕНИЕ 5

I. ПЪЛНО ДИСКОВО КРИПТИРАНЕ 5

1. Общи особености на сигурността на пълното дисково криптиране 5
2. Уязвимости на дисковете след физическо достъпване 6
3. Видове атаки на софтуерно-базираното пълно дисково криптиране 6

3.1. Атаки експлоатиращи DMA 6
3.2. Атаки от типа „Cold boot“ 7
3.3. Атаки от типа Evil Maid 7

II. ОБЩИ ОСОБЕНОСТИ В СИГУРНОСТТА НА ХАРДУЕРНО-БАЗИРАНОТО ПЪЛНО ДИСКОВО КРИПТИРАНЕ 8

a. Сигурност на ATA 8
b. Самокриптиращи се дискове (СКД) 8
c. Opal Security Subsystem Class 9

III. ВИДОВЕ АТАКИ НА ХАРДУЕРНО-БАЗИРАНОТО ПЪЛНО ДИСКОВО КРИПТИРАНЕ 9

1. Атаки от типа Hot Plug 9

1.1. Концепция за атаките 9
1.2. Настолни и сървърни системи 9
1.3. Лаптопи и suspend to Ram 10
1.4. Захранване 10
1.5. Получаване на ata пароли от Ram 10

2. Пригаждане на известни атаки с цел пробиване сигурността на самокриптиращите се дискове 11

2.1. Evil Maid атаки срещу СКД 11
2.2. DMA атаки срещу СКД 11
2.3. Cold boot атаки на СКД 12

IV. МЕРКИ ЗА ПРОТИВОДЕЙСТВИЕ 13

a. Потребителско ниво 13
b. Операционна система 13
c. BIOS/дънна платка 13
d. Ниво СКД 13

ЗАКЛЮЧЕНИЕ 13

ЛИТЕРАТУРА 14

ЧЕСТО ИЗПОЛЗВАНИ СЪКРАЩЕНИЯ

ПДК – пълно дисково криптиране

СКД – самокриптиращ(и) се диск(ове)

MBR – сектор за начално зареждане на операционната система (master bood record)

DMA – директен достъп до паметта

ВЪВЕДЕНИЕ

В наши дни чувствителните данни на една организация се намират върху мобилни устройства и сървъри на различни точки по света и подлежат на постоянни атаки. Освен това сървърните системи могат да бъдат конфискувани от правораздавателните органи. Задаването на пароли на ниво операционна система и BIOS е неефективно за защита на данните срещу непозволен достъп. При такива сценарии криптирането на данните се явява необходимост.

Изследване на Symantec[1] показва, че през 2011 г. 34% от случаите на непозволен достъп до данни е свързано с кражбата на физически устройства, каквито са лаптопите. Според проучване на Ponemon Institute[2] от април 2013 г. 36% от организациите в САЩ използват дискове с функция за самокриптиране, но при 77% от тях едва 5% (лаптопи и настолни компютри) имат активирана тази функция. Тук възниква въпросът колко сигурни са самокриптиращите дискове и заслужава ли си да заменят други средства за защита?

I. ПЪЛНО ДИСКОВО КРИПТИРАНЕ

1. ОБЩИ ОСОБЕНОСТИ НА СИГУРНОСТТА НА ПЪЛНОТО ДИСКОВО КРИПТИРАНЕ

Пълното дисково криптиране (ПДК) означава извършването на криптиране върху целия диск, за да може да се подсили сигурността на данните в случаи на физическо загубване, кражба на диск или цялата машина. За тази цел, прекият процес за постигане и поддържане на ПДК се извършва или от операционната система, или от специален хардуер, така че ПДК накратко може да бъде разделено на софтуерно-базирано и хардуерно-базирано. Докато софтуерно-базираните решения като Bitlocker и TrueCrypt[3] съществуват повече от десетилетие за крайните потребители, разпространението на хардуерно-базираните алтернативи се налагат от по-скоро, с получаването на по-широко разпространение на SSD дисковете. Тези дискове съхраняват криптографските си ключове в контролера на диска или на криптиран дял на самия диск[4] и по този начин ключовете за криптиране никога не преминават през паметта на процесора или оперативната памет (RAM) на компютъра. Поради тази причина тези дискове често биват определяни като самокриптиращи се.

Освен безспорните предимства от използването на тази техника, сред които са поддръжката, прозрачността от операционната система и значителната полза по отношение на производителността, самокриптиращите се дискове (СКД) обикновено се считат за по-сигурни, отколкото дисковете, защитени със софтуерно-базирано криптиране. Така например, според проучването на Ponemon Institute, в САЩ само 24% от запитаните считат, че СКД не са по-сигурни от софтуерно-базираното криптиране. На същия въпрос във Великобритания на такова мнение са 17%, а в Германия – 18%.

---

1 Sean Michael Kerner, *Symantec: Attacks On the Rise, But Spam and Botnets Down*, eSecurity Planet, 30 April 2012, at http://www.esecurityplanet.com/hackers/symantec-attacks-on-the-rise-but-spam-and-botnets-down.htm l.

2 The TCO of Software vs. Hardware-based Full Disk Encryption.

3 На 28. май 2014 г. сайтът на TrueCrypt оповести, че разработката на софтуера престава, а неговите потребители бяха призовани да спрат да го използват, заради възможни проблеми със сигурността.

4 J.D. Hietala, Hardware versus Software. A Usability Comparison of Software-Based Encryption with Seagate DriveTrust Hardware-Based Encryption, A SANS Whitepaper, September 2007.

Аргументите в ползва на СКД обикновено са следните: Първо, дизайнът на СКД винаги позволява ПДК, включително на сектора за начално зареждане (master bood record - MBR). При софтуерно-базираното криптиране MBR се представя винаги некриптиран, за да може операционната система да се зареди, което подлага компютъра на риск от атака, наречена *Evil Maid*[5]. На второ място, при СКД ключът за криптиране не постъпва в RAM паметта, което премахва възможността да се извърши атака в това направление. Подобни атаки са възможни при софтуерно-базираното криптиране под формата на *cold boot*[6] и DMA[7] атаки.

2. УЯЗВИМОСТИ НА ДИСКОВЕТЕ СЛЕД ФИЗИЧЕСКО ДОСТЪПВАНЕ

За успешно намиране на ключа за криптиране, атаките, провеждани на СКД, изискват физически достъп до устройствата. Другите атаки се съсредоточават върху механизмите за защита на операционната система или използват средствата за социално инженерство, за да бъде измамен потребителя и да разкрие паролата. Тук няма да се разглеждат атаки, които не изискват физически достъп до хардуера и проникват в системите посредством зловреден код през мрежата. Криптирането на дискове е механизъм за защита на конфиденциалността на данните след кражба на диска, загубата му или преоразмеряването му.

Възможността за провеждане на повечето атаки изисква системата да работи или да е в standby режим. Ако компютърът работи се допуска, че той е заключен, защото в противен случай достъпът до данни става по тривиален начин. Най-обичайният сценарий на атаки на физическия достъп е чрез сървърите и настолните компютри, които работят, но са заключени. Обикновено лаптопите се считат за основна цел на тези атаки, тъй като те често биват изгубвани и откраднати на публични места, например на летища. Въпреки това, такива атаки могат да бъдат осъществени и върху настолни машини и сървъри. Те например могат да бъдат атакувани от хакери, които имат физически достъп до машините или да бъдат конфискувани от органите на реда.

Настоящата работа не дава отговор на въпроса до каква степен съществуващите СКД са засегнати от атаки с физически достъп до тях. Тук ще се покаже, че СКД не са защитени от много видове атаки, въпреки, че рекламите на отделните производители може да твърдят обратното.

3. ВИДОВЕ АТАКИ НА СОФТУЕРНО-БАЗИРАНОТО ПЪЛНО ДИСКОВО КРИПТИРАНЕ

Тук ще разгранича три типа атаки с физически достъп срещу софтуерно-базираното ПДК, за да може да се придобие по-добра представа за хардуерно-базираното ПДК.

3.1. Атаки експлоатиращи DMA

Една от основните уязвимости на софтуерно-базираните системи произхожда от факта, че ключовете за криптиране се съхраняват в основната памет, която е възможно да бъде прочетена чрез директен достъп (direct memory access – DMA). Освен това атаките на този принцип могат дори да правят записи в паметта. В интернет свободно могат да се

---

5 Schneier on Security, 23 October 2009, https://www.schneier.com/blog/archives/2009/10/evil_maid_attac.html.

6 *Lest We Remember: Cold Boot Attacks on Encryption Keys*, 2008 USENIX Security Symposium, 21 February 2008, at http://citpsite.s3-website-us-east-1.amazonaws.com/oldsite-htdocs/pub/coldboot.pdf.

7 Patrick Stewin and Iurii Bystrov, *Understanding DMA Malware*, Security in Telecommunications, Technische Universit□at Berlin, 2012, at http://stewin.org/papers/dimvap15-stewin.pdf.

намерят подходи за атака над Bitlocker[8]. По принцип всички интерфейси за DMA имат същите уязвимости, включително PCI и ExpressCard[9]. Възможна мярка за противодействие срещу този вид заплаха се постига чрез технологията IOMMU[10], но тя не е широко разпространена в днешния хардуер.

3.2. Атаки от типа „Cold boot“

Тези атаки, получили публичност през 2008 г., експлоатират главната памет за достъп до ключа за криптиране. Това се дължи на факта, че съдържанието в паметта се изгубва постепенно във времето, не наведнъж. Това позволява на атакуващия да възстанови ключ от оперативната памет чрез стартиране на компютъра с малка операционна система на USB стик. За разлика от DMA атаките, за които е необходимо да се използва специален DMA интерфейс за връзка, cold boot атаките са общо приложими и противодействието срещу тях е по-трудно. И до днес всички широко разпространени софтуерно-базирани решения за ПДК са уязвими на този вид атаки, включително BitLocker, TrueCrypt и File Vault.

Възможно решение за предотвратяване на атаките от този вид е предложено в научната литература и се изразява в това да се преместят ключовете за криптиране от главната памет в кеша на процесора или в регистрите на му[11]. Пачът за Linux „TRESOR” съхранява ключовете в дебъг регистрите на процесора, но въпреки това не успява да удържи на DMA атаки.[12]

3.3. Атаки от типа Evil Maid

Тези атаки са открити през 2009 г. и са възможни заради некриптирания сектор за начално зареждане (MBR), който не се криптира, за да може да стартира операционната система. Поради тази причина такива сектори могат да бъдат изменяни лесно, например чрез вкарването на кийлогъри. Атаки от този тип се срещат и с наименованието bootkits. Друга особеност на този вид атаки е, че те изискват достъп до атакувания компютър два пъти: преди въвеждането на паролата и след това. Чрез първата физическа атака атакуващият инсталира кийлогър върху MBR сектора и чрез повторния достъп извлича паролата.

Тези атаки могат частично да бъдат смекчени чрез стандарта trusted platform module (TPM). Други решения са предложени от Жоана Рутковска в нейния блог.[13]

---

8 Sven Turpe, Andreas Poller, Jan Steffan, Jan-Peter Stotz, and Jan Trukenmuller, *Attacking the BitLocker Boot Process*, Fraunhofer Institute for Secure Information Technology (SIT), Darmstadt, Germany, 2009, at http://testlab.sit.fraunhofer.de/downloads/Publications/Attacking_the_BitLocker_Boot_Process_Trust2009.pdf.

9 *Adventures with Daisy in Thunderbolt-DMA-land: Hacking Macs through the Thunderbolt interface,* Break&Enter.org, Security News, Tools & Methodology, 6 February 2012, at http://www.breaknenter.org/2012/02/adventures-with-daisy-in-thunderbolt-dma-land-hacking-macs-through-the-thunderbolt-interface/

10 *A Password Is Not Enough 3: Trusted Platform Module as a Means for Measured Boot*, Privacy Pc.com, 10 March 2014, at http://privacy-pc.com/articles/a-password-is-not-enough-3-trusted-platform-module-as-a-means-for-measured-boot.html.

11 Tilo Muller, Felix C. Freiling, Andreas Dewald, *TRESOR Runs Encryption Securely Outside RAM*, Department of Computer Science University of Erlangen, Laboratory for Dependable Distributed Systems University of Mannheim, 2012, at https://www.usenix.org/legacy/events/sec11/tech/full_papers/Muller.pdf.

12 Erik-Oliver Blass, William Robertson, *TRESOR-HUNT: Attacking CPU-Bound Encryptio*, Northeastern University, 2012, at https://www.acsac.org/2012/openconf/modules/request.php?module=oc_program&action= view.php&a=&id=237&type=4&OPENCONF=8leugbu5he7redddl4p30uj4o0.

13 *Anti Evil Maid*, The Invisible Things blog.com, 07 September 2011, at http://theinvisiblethings.blogspot.com/2011/09/anti-evil-maid.html.

II. ОБЩИ ОСОБЕНОСТИ В СИГУРНОСТТА НА ХАРДУЕРНО-БАЗИРАНОТО ПЪЛНО ДИСКОВО КРИПТИРАНЕ

Дисковете от типа SSD (Solid-state drvies) започват все по-широко да се налагат сред потребителите, постепенно изместващи добре познатите HDD (hard disk drives). Те са издръжливи на механични удари и до няколко пъти по-бързи от HDD. Освен това съвременните производители на SSD ги проектират с функционалността да се само-криптират. Това често е наричано drive-level encryption. Въпреки широкото разпространение на SSD, подобно криптиране съществува и при отделни модели HDD.

A. Сигурност на ATA

ATA (Advanced Technology Attachment) е стандартен интерфейс за свързване на устройства за съхранение на информация и масовото му използване започва от 90-те години на XX век. Съвременният интерфейс SATA (Serial ATA), който се използва за свързване на дисковете за съхранение на данни в потребителския сегмент е стан-дартизиран през 2003 г. и от тогава претърпява няколко ревизии. ATA дисковете имат способността да се заключват и да останат „недостъпни“, докато не се въведе правилната парола, но това заключване не включва обезателно криптиране.

Сигурността на ATA позволява задаването на два типа парола – Потребителска и Главна, както и две нива на сигурност: Високо и Максимално. На ниво Високо паролата за Потребител и Главната парола могат да бъдат използвани единично за отключване на диска. На Максимално ниво Главната парола може да бъде използвана само за надеждно изтриване на съдържанието на диска, както и за възстановяване на Потребителската парола, но без да има възможност записаното съдържание да бъде прочетено. С други думи Главната парола позволява на администратора на системата (фирмата или производителя) да възстановят заводските настройки на диска, в случай на изгубване на паролата. И двата вида пароли са дълги 32 байта.

Чистите пароли за ATA дават малко по-голяма сигурност от паролата за BIOS и паролата за операционната система, тъй като ATA паролата не предполага от само себе си, че дискът е криптиран. Поради тази причина SATA заключването не трябва да се бърка със СКД. За да премахне паролата за ATA, атакуващият може да пропусне чипа на контролера на диска и да достъпи паметта директно. Това обикновено изисква използването на специален за целта хардуер, но пълен достъп до диска винаги може да бъде получен. За да се завърши физическото ниво на сигурност е необходимо това заключване да се обвърже с криптиране на drive-level.

B. Самокриптиращи се дискове (СКД)

Както беше споменато производителите на SSD започнаха да включват в спецификациите на своите продукти способността да извършват вградено в тях криптиране. Тези модели използват AES стандарта, за да криптират данните. Например дисковете Intel SSD 320 използват AES-128, а Intel SSD 520 – AES-256.

Всеки СКД има уникален ключ за криптиране, който е генериран по ентропични методи[14] от самия диск. Този ключ се нарича media encryption key (MEK), известен и като data encryption key (DEK). MEK се използва, за да криптира потребителските данни на диска, но с помощта на ключа за криптографски ключ (key encryption key - KEK). Ключовете KEK се дават от Потребителските пароли. Криптираните дискове стартират заключени докато не се въведе правилната парола. Повторното криптиране бива избегнато, тъй като само MEK трябва да бъде криптиран наново с KEK, в случай, че паролата бъде сменена. Задаването на нова парола или премахването на паролата също не изисква дълго криптиране или декриптиране.

[14] Дефиниция на Ентропия, Whatis.com, 2014, at http://whatis.techtarget.com/definition/password-entropy.

Задаването на парола за СКД става по няколко начина, много често през BIOS. Много лаптопи имат вградена поддръжка на командите за сигурност за ATA и затова е естествено повечето производители на СКД да използват тази инфраструктура за автентификация.

C. Opal Security Subsystem Class

СКД могат да бъдат базирани и на друг стандарт, известен като Opal Security Subsystem Class. Той дава набор от спецификации, с които производителите на СКД могат да се съобразят. Този стандарт предлага друг начин за автентификация: когато BIOS изиска MBR от диска, последният отговаря, показвайки записа за начално стартиране. Записът за начално стартиране изисква от потребителя права за вписване. Не всички производители на дискове обаче поддържат този стандарт във всички си модели.

III. ВИДОВЕ АТАКИ НА ХАРДУЕРНО-БАЗИРАНОТО ПЪЛНО ДИСКОВО КРИПТИРАНЕ

1. АТАКИ ОТ ТИПА HOT PLUG

1.1. Концепция за атаките

Тези атаки са вдъхновени от един от вариантите за провеждане на cold boot атака. При него чиповете за RAM се отстраняват от работещия компютър и след това се включват към друг компютър, за да се извлече от тях информацията. Но тъй като би било безсмислено да се извадят RAM модулите когато говорим за хардуерно-базираното ПДК, ще изберем да направим това със самия диск. Този подход се оказва ефективен при всички СКД.

В този случай се експлоатира уязвимостта в СКД, че той не засича дали SATA кабелът е изваден докато захранващият кабел продължава да го захранва. СКД се заключва само когато захранването му е прекъснато, но остава отключен, ако се прекъсне връзката за пренос на данни. Това обстоятелство може да доведе до следния сценарий: Ако имаме физически достъп до работещ компютър можем да извадим SATA кабела и да свържем диска с кабел до друг компютър. По време на този процес собственият компютър служи като източник на електрическо захранване за диска. Вторият компютър, който е управляван от атакуващия, прехваща данните. Операционната система на оригиналния компютър се срива със „син“ екран. Ако компютърът на атакуващия поддържа „hot-plug“ SATA, дискът може да бъде прочетен директно. Ако това не стане, може да се наложи компютърът да бъде рестартиран. При всеки случай „hot-plug“ SATA не е изискване за извършване на атаката и достъпът до данните се получава без изискване за въвеждане на парола.

Названието „hot-plug атака“ идва от факта, че този тип атака поставя изискване дискът да работи и да е отключен. Системите, при които дискът не работи и е заключен, не могат да бъдат атакувани по този метод. Системите със СКД се оказват освен това по-уязвими отколкото тези със софтуерно ПДК, заради лесната и ефективността при провеждане на такива атаки. В този смисъл СКД се държат като самодекриптиращи се дискове, вместо самокриптиращи се.

1.2. Настолни и сървърни системи

На работещи компютри като настолните системи и сървърите hot plug атаките имат преимущества пред cold boot и DMA атаките, тъй като те могат да бъдат проведени независимо от настройките в BIOS и допълнителни DMA интерфейси. Настройки като „парола при начално зареждане“ и „Ред на стартиране на устройствата – boot device order“ не оказват влияние върху hot plug атаките. Освен това не се изисква използването на DMA порт. Тъй като сървърите работят постоянно те могат да бъдат перфектна цел за hot plug

атаки. Това може да бъде от полза за органите на реда, които изпълняват заповед за претърсване на сървърни клъстери. Дългите SATA кабели допълнително улесняват провеждането на такава атака.

1.3. Лаптопи и suspend to Ram[15]

Лаптопите са считани за по-критичен хардуер по отношение на защитата с ПДК, тъй като те често са изложени на риск от кражба. За разлика от сървърните клъстери, които обикновено са защитени с някаква форма на физическа защита, например охранители, лаптопите могат бързо да попаднат у злонамерени хора. При лаптопите обаче кабелите за захранване и данни не могат да бъдат толкова лесно извадени за целите на експлоатация на уязвимостите.

Друга трудност произтича от това, че те не работят постоянно, както сървърите. Те биват открадвани или изключени, или в режим standby. Когато са в режим standby, това обикновено означава, че те са в режим ACPI S3, т.е. suspend to RAM. В този режим СКД е изключен и е заключен. Същото се отнася за Hibernation режима, т.е. ACPI S4, или suspend to disk.

Уязвимостта произтича от режима ACPI S3, който съществува практически при всички лаптопи. Те изискват ATA парола, за да стартират, но дискът се отключва автоматично след събуждане от S3. Това може да доведе до следната атака: когато дискът е изключен и е заключен, той може да бъде изваден от шасито на лаптопа. Веднъж изваден можем да свържем удължаващ SATA кабел и кабел за захранване към друг компютър. След това „събуждаме“ диска и СКД автоматично се отключва. По-нататък атаката продължава по начин, описан вече за настолните и сървърните компютри: изваждаме SATA кабела и го поставяме във втори компютър, за да достъпим данните.

Тъй като атакуващите могат да вкарат работещите лаптопи в sleep режим, което често става чрез затваряне на капака на монитора, то работещите лаптопи са също засегнати от тази уязвимост. Windows и Linux позволяват пускането на лаптопа в sleep режим без допълнителни привилегии. В описания случай самият СКД е сигурен, но системата като цяло не е.

1.4. Захранване

Някои нови лаптопи засичат дали СКД е изваден от захранването си по време на S3. За разлика от RAM паметта, където съдържанието в паметта се запазва в продължение на няколко секунди без модулът да е включен към захранване, тези видове СКД се заключват веднага след отстраняването на кабела. В случаите когато standby-базираните атаки изискват изваждането на SATA кабела и този на захранването, атаката е безуспешна.

1.5. Получаване на ata пароли от Ram

Интересен е въпросът дали СКД може да бъде отключен посредством извличане на криптографския ключ от RAM паметта[16]. Тези дискове могат да бъдат отключени от спящ режим само чрез команда подадена от ATA интерфейса, което предполага, че ATA паролата трябва да се намира в RAM или VRAM, тъй като други компоненти не биват захранвани. По този начин паролата би трябвало да е достъпна в паметта на компютъра, както това е възможно за софтуерното ПДК, напр. при TrueCrypt[17]. Спецификация на СКД по данни на

---

15 *Suspend and Hibernate*, Archlinux.org, 2014, at https://wiki.archlinux.org/index.php/Suspend_and_Hibernate.

16 *Security risk: Sensitive data can be harvested from a PC even if it is in standby mode, experts say*, ScienceDaily.com, 10 August 2012, at http://www.sciencedaily.com/releases/2012/08/120810083611.htm.

17 *Unencrypted Data in RAM*, 2014, at http://www.truecrypt.org/docs/unencrypted-data-in-ram.

Lenovo[18] показват, че тази уязвимост изглежда не е налична за СКД, използващи вече споменатия стандарт OPAL за криптиране, а вероятно не само при него.

2. ПРИГАЖДАНЕ НА ИЗВЕСТНИ АТАКИ С ЦЕЛ ПРОБИВАНЕ СИГУРНОСТТА НА САМОКРИПТИРАЩИТЕ СЕ ДИСКОВЕ.

След като видяхме, че hot plug атаките имат висока степен на приложимост можем да се запитаме дали и в какъв вид описаните атаки за софтуерно-базираното ПДК са възможни. Тук ще покажем, че адаптации на атаките срещу софтуерно-базираното ПДК или техният оригинален вид са приложими и при хардуерно-базираното ПДК.

2.1. Evil Maid атаки срещу СКД

Както беше споменато атаките от типа Evil Maid не изискват системата да бъде включена или да бъде в режим standby. Атаката при софтуерно-базираното ПДК се осъществява със замяна на оригиналния MBR с друга, изменена версия, която има допълнителната функционалност да прихваща натискането на клавиши. Така на атакуващия е необходимо 2 пъти да достъпи компютъра на жертвата: първо, за да инсталира променения MBR и след това – за да извлече паролата на жертвата.

При софтуерно-базираното криптиране това е възможно, защото MBR никога не е криптиран. При хардуерно-базираното криптиране, обаче, MBR се криптира и атаката в този ѝ вид не е приложима. Тя обаче може да бъде променена. За целта разиграваме следния сценарий:

Атакуващият влиза с взлом в хотелската стая на атакувания обект и заменя неговия СКД в лаптопа с друг. След като потребителят се прибере и включи лаптопа си той вижда начален екран за въвеждане на парола, много подобен на неговия и въвежда паролата си. След това паролата се изпраща по мрежата до атакуващия.

Разбира се, жертвата ще стане подозрителна когато види, че операционната система и потребителските данни не могат да бъдат декриптирани, но ще е твърде късно, тъй като атакуващият вече притежава неговия СКД и парола. Заменението диск допълнително се самоизтрива, за да не останат следи. Ако се използва СКД от същия модел жертвата може дори да не забележи промяната и да помисли, че СКД се е повредил.

В сравнение с традиционната атака, тази не изисква два пъти да се достъпва лаптопът на атакувания, тъй като той е свързан в мрежа. С нарасналата употреба на безжични мрежи тази свързаност може да се осъществи дори с личен hotspot на атакуващия.

Подобна атака на манипулиране на началното зареждане може да се осъществи след включване на малък USB стик или чрез рефлашване на BIOS. В друг случай самият лаптоп може да бъде заменен.

2.2. DMA атаки срещу СКД

Вече беше споменато, че при DMA атаките целта е компрометиране на главната памет с цел извличане на криптографския ключ. В други случаи атакуващият може да пише в паметта и по този начин да я измени по свое желание. Това може например да доведе от отключване на заключен екран на операционната система, както това е доказано за Windows 7, криптиран с BitLocker[19].

---

[18] *SecureDoc™ for Lenovo*, WinMagic Data Security, 2012 at http://www.lenovo.com/us/en/PDFs/lenovo_securedoc_disk_encryption.pdf.

[19] Benjamin Böck, *Firewire-based Physical Security Attacks on Windows 7, EFS and BitLocker*, Security Research Lab Secure Business Austria, 2009, at http://www.net-security.org/dl/articles/windows7_firewire_physical_attacks.pdf.

При атакуване на СКД първият вариант на DMA атака (достъпване на RAM) би бил неуспешен, тъй като ключът за криптиране не е в RAM. Но вторият вариант (отключване на заключен екран) работи по същия начин. Условието за провеждане на успешна атака от този вид все пак изисква атакуваният компютър да работи или да е в режим standby. Засегнати са Windows, Mac OS X и някои Linux дистрибуции.

Уязвимостта, която се експлоатира, е заради вградения FireWire[20] порт или която и да е Express карта[21]. При нея Windows инсталира драйвърите за FireWire на заден план, докато е заключен. Адаптер на FireWire към Express карта може да се използва със същия ефект. Тази уязвимост се оказва неприложима при настолните конфигурации, въпреки, че PCIe слотът на дънните платки по спецификации поддържа hot plug функционалност. Причината е, че или операционната система, или самата дънна платка не поддържа hot plug и поради тази причина е трудно да се демонстрира атака без FireWire порт. Thunderbold интерфейсът също позволява трансфер на данни от DMA[22].

2.3. Cold boot атаки на СКД

Атаките cold boot са типично приложими за софтуерно-базираното ПДК. Основната идея зад тези атаки е да се получи достъп до ключа в главната памет след като системата е рестартирана с малък USB стик или оптичен диск. Въпреки масовата представа, че след изключване на компютъра данните от паметта веднага изчезват, те в действително се запазват за около 30 секунди или след минути, ако преди това модулите за памет са охладени. Рестартирането на системата гарантира паметта да не остарее.

Рестартирането на атакуваната система, за да се извлекат данни от RAM изглежда безсмислено при СКД, тъй като ключът за криптиране не е се запазва там. Много от лаптопите обаче не биха питали за парола след рестарта и атаката върху тях става тривиална. Все пак някои лаптопи имат BIOS настройка, която позволява активирането на ATA парола при рестартиране. Това означава, че при лаптопите може да отсъства една такава необходима настройка. Уязвимите системи позволяват стартиране на Linux live операционна система от външен диск и от там да се прикачат дяловете на все още отключения СКД. Тази атака се оказва по-проста и от hot plug атаката, но въпреки това ефективно пробива защитата на много СКД. Отново, СКД се държи като „самодекриптиращ се“ диск.

При рестартиране на системите много дискове показват уязвимостта да остават отключени. В този смисъл рестартирането от бутон и рестартирането от операционната система постига същия ефект. Тъй като лаптопите нямат отделен бутон за рестартиране процесът може да се извърши чрез свързване на два пина на дънната платка. Ако настройките на BIOS не ни позволяват да стартираме външни устройства, можем да свържем втори твърд диск (но това по всяка вероятност няма да е възможно на лаптопи, а на настолни компютри). Както се разбира, тази атака зависи от елементи, които често не са предвидими – BIOS настройките и хардуерната окомплектовка.

В други лаптопи рестартирането води до заключване на диска, което може да се дължи на софтуерна настройка и по този начин се намалява възможността за реализация на този вид атака. Все пак и този защитен механизъм може да бъде преодолян, но това изисква повече прецизност и бързина на действие: След стартиране на процеса за рестартиране на компютъра малко преди самото рестартиране може да се извади SATA кабелът, за да се предотврати заключването на диска. Причината за това е, че СКД не се заключва ако не е свързан с компютъра по времето, когато се изпраща ATA командата за заключването му. Това по всяка вероятност е обща уязвимост на СКД.

---

20 *FireWire definition*, SearchNetworking, April 2007, http://searchnetworking.techtarget.com/definition/FireWire.

21 *ExpressCard*, definition, Wikipedia.org, 2014, at http://en.wikipedia.org/wiki/ExpressCard.

22 *Adventures with Daisy in Thunderbolt-DMA-land: Hacking Macs through the Thunderbolt interface,* Break & Enter, 6 February 2012, at http://www.breaknenter.org/2012/02/adventures-with-daisy-in-thunderbolt-dma-land-hacking-macs-through-the-thunderbolt-interface/

IV. МЕРКИ ЗА ПРОТИВОДЕЙСТВИЕ

Най-ефективната мярка за противодействие на атаки срещу СКД е компютърът винаги да се държи напълно изключен (shutted down) и физически заключен. Тук започваме да говорим за физическа защита, което излиза извън рамките на настоящата работа. Поради тази причина ще спомена за нивата на защита, които трябва да се вземат предвид: потребителско ниво, операционна система, BIOS/дънна платка и самите СКД.

A. Потребителско ниво

Противодействието трябва да се гарантира на ниво настройки на BIOS и задаването на парола на BIOS, което е нещо различно от паролата за диск. Потребителите ще трябва да въвеждат две различни пароли при стартиране на компютъра, но по този начин ще бъдат преодолени атаките от типа cold boot.

B. Операционна система

За справяне с FireWire атаки може да се закупи компютър без DMA портове. Това обаче може да е твърде крайно решение за много потребители. Вместо това DMA атаките могат да се предотвратят на ниво операционна система. За тази цел DMA трансферите на данни могат да бъдат филтрирани с помощта на IOMMU[23], което е възможно благодарение на технологията за виртуализация на директен I/O.[24]

C. BIOS/дънна платка

Производителите на BIOS трябва да предприемат мерки за защита при хардуерно-базирано ПДК, така че SATA паролите да не бъдат съхранявани в RAM или NVRAM. Когато един СКД спре да бъде захранван той не бива да може да бъде отключен автоматично и потребителят винаги трябва да бъде питан за въвеждане на парола. Това вече съществува при някои дънни платки.

D. Ниво СКД

За справяне с атаки hotplug трябва да се разработи функционалност за заключване на СКД след отстраняване на SATA кабела. На този етап СКД се заключват само когато токът до тях е прекъснат. Една възможна мярка за това е когато СКД обменят данни и се захранват от един единствен конектор. Това е възможно например за RAM модулите и за PCLe устройствата. Вече съществуват SSD дискове, които се свързват посредством PCLe за по-голяма производителност.

ЗАКЛЮЧЕНИЕ

Настоящата работа разгледа няколко възможности за преодоляване на защитата на самокриптиращите се дискове. Беше онагледено, че самокриптиращите дискове, както дисковете криптирани със софтуер, който е инсталиран от операционната система, не са защитени от познати атаки адаптирани за тях, както и от нови атаки. Дисковете са уязвими на атаки от вида DMA, Evil Made, варианти на cold boot атаки и на нови атаки, които бяха наречени hot plug. Степента на уязвимост зависи от хардуерната окомплектовка и функционалностите на BIOS, операционната система и др.

---

[23] *IOMMU definition*, Wikipedia.org, 2014, at http://en.wikipedia.org/wiki/IOMMU.

[24] *Intel® Virtualization Technology for Directed I/O (VT-d): Enhancing Intel platforms for efficient virtualization of I/O devices*, Software Intel.com, 03 May 2012, at https://software.intel.com/en-us/articles/intel-virtualization-technology-for-directed-io-vt-d-enhancing-intel-platforms-for-efficient-virtualization-of-io-devices.

ЛИТЕРАТУРА

1. Sean Michael Kerner, *Symantec: Attacks On the Rise, But Spam and Botnets Down*, eSecurity Planet, 30 April 2012, http://www.esecurityplanet.com/hackers/symantec-attacks-on-the-rise-but-spam-and-botnets-down.html.

2. J.D. Hietala, *Hardware versus Software. A Usability Comparison of Software-Based Encryption with Seagate DriveTrust Hardware-Based Encryption*, A SANS Whitepaper, September 2007.

3. Schneier on Security, 23 October 2009, https://www.schneier.com/blog/archives/2009/10/evil_maid_attac.html.

4. *Lest We Remember: Cold Boot Attacks on Encryption Keys*, 2008 USENIX Security Symposium, 21 February 2008, http://citpsite.s3-website-us-east-1.amazonaws.com/oldsite-htdocs/pub/coldboot.pdf.

5. Patrick Stewin and Iurii Bystrov, *Understanding DMA Malware*, Security in Telecommunications, Technische Universitat Berlin, 2012, http://stewin.org/papers/dimvap15-stewin.pdf.

6. Sven Turpe, Andreas Poller, Jan Steffan, Jan-Peter Stotz, and Jan Trukenmuller, *Attacking the BitLocker Boot Process*, Fraunhofer Institute for Secure Information Technology (SIT), Darmstadt, Germany, 2009, http://testlab.sit.fraunhofer.de/downloads/Publications/Attacking_the_BitLocker_Boot_Process_Trust2009.pdf.

7. *Adventures with Daisy in Thunderbolt-DMA-land: Hacking Macs through the Thunderbolt interface,* Break&Enter.org, Security News, Tools & Methodology, 6 February 2012, http://www.breaknenter.org/2012/02/adventures-with-daisy-in-thunderbolt-dma-land-hacking-macs-through-the-thunderbolt-interface/.

8. *A Password Is Not Enough 3: Trusted Platform Module as a Means for Measured Boot*, Privacy Pc.com, 10 March 2014, http://privacy-pc.com/articles/a-password-is-not-enough-3-trusted-platform-module-as-a-means-for-measured-boot.html.

9. Tilo Muller, Felix C. Freiling, Andreas Dewald, *TRESOR Runs Encryption Securely Outside RAM*, Department of Computer Science University of Erlangen, Laboratory for Dependable Distributed Systems University of Mannheim, 2012, https://www.usenix.org/legacy/events/sec11/tech/full_papers/Muller.pdf.

10. Erik-Oliver Blass, William Robertson, *TRESOR-HUNT: Attacking CPU-Bound Encryptio*, Northeastern University, 2012, https://www.acsac.org/2012/openconf/__modules/request.php?module=oc_program&action=view.php&a=&id=237&type=4&OPENCONF=8leugbu5he7redddl4p30uj4o0.

11. *Anti Evil Maid*, The Invisible Things blog.com, 07 September 2011, http://theinvisiblethings.blogspot.com/ 2011/09/anti-evil-maid.html.

12. Дефиниция на Ентропия, Whatis.com, 2014, http://whatis.techtarget.com/definition/password-entropy.

13. *Suspend and Hibernate*, Archlinux.org, 2014, https://wiki.archlinux.org/index.php/Suspend_and_Hibernate.

14. *Security risk: Sensitive data can be harvested from a PC even if it is in standby mode, experts say*, ScienceDaily.com, 10 August 2012, http://www.sciencedaily.com/releases/2012/08/120810083611.htm.

15. *Unencrypted Data in RAM*, 2014, http://www.truecrypt.org/docs/unencrypted-data-in-ram

16. *SecureDoc™ for Lenovo*, WinMagic Data Security, 2012 http://www.lenovo.com/us/en/PDFs/lenovo_securedoc_disk_encryption.pdf.

17. Benjamin Böck, *Firewire-based Physical Security Attacks on Windows 7, EFS and BitLocker*, Security Research Lab Secure Business Austria, 2009, http://www.net-security.org/dl/articles/windows7_firewire_physical_attacks.pdf.

18. *FireWire definition*, SearchNetworking, April 2007, http://searchnetworking.techtarget.com/definition/FireWire.

19. *ExpressCard*, definition, Wikipedia.org, 2014, http://en.wikipedia.org/wiki/ExpressCard.

20. *IOMMU definition*, Wikipedia.org, 2014, http://en.wikipedia.org/wiki/IOMMU.

21. *Intel® Virtualization Technology for Directed I/O (VT-d): Enhancing Intel platforms for efficient virtualization of I/O devices*, Software Intel.com, 03 May 2012, https://software.intel.com/en-us/articles/intel-virtualization-technology-for-directed-io-vt-d-enhancing-intel-platforms-for-efficient-virtualization-of-io-devices.