Disco Duro Cifrado ¿Datos seguros?

Espinosa Cortez, Giselle
Universidad Autónoma de México
Facultad de Ingeniería
espinosacortezgiselle@gmail.com

Resumen- El cifrado de disco duro, es una forma segura en la que nuestros equipos protegen la información almacenada en él. Cifrando todos los archivos y descifrando solo aquellos a los que queremos acceder,esto se hace a través de softwares confiables que ya nos proporciona nuestro equipo solo necesitamos una contraseña que nos pemirte acceder. En este caso solo hablaremos de bitlocker el software de cifrado de disco de Windows y como nuestros datos están expuestos a pesar de implementar el cifrado del disco a nuestro equipo.

Contrario a lo que se piensa la RAM no es tan volátil esto genera que nuestros datos queden expuestos a atacantes por un pequeño tiempo que puede expandirse si enfriamos el módulo de DRAM, esto permite al ataque de arranque en frio acceder y no solo hay una forma en la que puede burlar al sistema sino tres que propuso Halderman et al [2] y a pesar de ser un articulo viejo se siguen usando para poner a prueba las más recientes DRAM's que utilizan nuestros equipos.

I.INTRODUCCIÓN

Uno de los pensamientos más comunes es que el poner una contraseña a nivel usuario no permitirá a otras personas acceder a nuestro equipo y no es importante por ahora para nosotros ya que no guardamos información delicada en nuestros equipos, pero pensemos que es así como tenemos información sumamente delicada. Lo primero que pensaríamos es cifrar nuestro disco ya que esto permitiría tener mis documentos inentendibles en caso de que alguien accediera a ellos y no tuviera la clave de cifrado, pero vamos más allá si roban mi computadora ya con esta protección ¿Mis datos siguen seguros? La respuesta es no, ya que existe un ataque que burla esa protección ya que digámoslo así accede por una puerta trasera, para poder llegar a las llaves de cifrado y urtarlas.

Esto se puede hacer a través de la RAM ya que aunque conceptualmente es volátil, es decir, todo desaparece cuando nosotros apagamos el equipo. En la realidad una celda DRAM es esencialmente un capacitor como sabemos un capacitor no se descarga de inmediato. El efecto de reminiscencia es causado por lo anterior y puede prolongarse a través del enfriamiento de este.

I. CIFRADO DEL DISCO DURO

Digamos que un día un ladrón llega a robar nuestro equipo y este quiere acceder a nuestros datos, probablemente pensaríamos no importa le puse contraseña a mi equipo, pero si quitan nuestro disco duro y lo colocan en otra unidad, nuestros datos ¿Siguen seguros? La respuesta es no.

Aquí es cuando utilizamos el cifrado de disco completo (FDE por sus siglas en ingles *Full Disk Encryption*) pues este se utiliza para mantener la privacidad de los datos de tu disco duro. Nosotros protegemos nuestros archivos cifrándolos a través de un software especializado (Bitlocker para Windows, FileVault para Mac OS y FUKS para Linux), ocultando cada uno de los archivos, por otro lado, cuando se requiere acceder a estos nosotros debemos colocar la llave maestra solo descifrando ese archivo y todos los demás continúan cifrados, esto se explica de la manera más genérica posible, evidentemente cifrar un disco es mucho más complejo.

Volvamos al ejemplo inicial, si un ladrón robara nuestra computadora ahora con el cifrado del disco completo ¿Podría seguir accediendo a nuestra unidad? Esta pregunta la contestaremos más adelante.

A. BitLocker

Conocida también como BitLocker Driver Encryption, diseñada para el uso de usuarios Windows esta disponible desde su versión Windows Vista. Utilizando bitlocker, los usuarios son inmunes a las amenazas de fugas de datos provocada por perdida, robo o eliminación incorrecta del disco duro [3].

BitLocker está diseñado para prevenir ataques fuera de línea[1], sin embargo, los ataques a Bitlocker se basan principalmente en el descifrado de clave o contraseña de desbloqueo [3]

1. Un ataque en el que el atacante obtiene algunos datos (normalmente al espiar la ejecución de un protocolo de autenticación o al penetrar en un sistema y robar archivos de seguridad) que puede analizar en un sistema de su elección [8]

Ataque de arranque en frio también conocido en inglés como cold boot atack es un método de ataque físico avanzado, mediante el cual se puede obtener la clave Bitlocker de la memoria [3].

II.ATAQUE DE ARRANQUE EN FRIO

Un ataque de arranque en frío[2] es un ataque físico que roba el contenido de la memoria en computadoras o sistemas portátiles con pantalla bloqueada. Para un ataque de arranque en frío, el atacante reinicia el sistema de destino y ejecuta un código de volcado de memoria malicioso en lugar de una secuencia de arranque regular. Luego, el código de volcado de memoria transfiere el contenido de la DRAM al atacante; así el atacante logra su propósito [6]

2. La definición de arranque en frío es un método de arranque para quita la energía del sistema y vuelve a suministrarla.

A. Remanencia

Si hacemos una comparación entre el disco duro y la RAM, podemos apreciar que esta última interviene en cada acción realizada en el sistema y que contiene más datos sensibles que el propio disco duro como, por ejemplo, las contraseñas introducidas, los historiales, así como ciertos datos que no figuran en el disco duro. [10]

La memoria no está encriptada y permite, de este modo, el acceso al sistema y su manipulación. Además, un ataque a la memoria principal es más discreto que la modificación de algún archivo en el disco, convirtiéndola en una víctima potencial. [10]

DRAMS suelen usarse como memoria principal en las computadoras modernas, conceptualmente, DRAM´s es volátil. Lo que significa que mantiene los contenidos almacenados solo cuando se suministra energía. Debido a su volatilidad, muchas personas tienden a creer que la DRAM es un medio de almacenamiento seguro para datos sensibles a la seguridad y la privacidad; cuando se desconecta físicamente de la placa base, el contenido no sería recuperable ya que se corta la energía. [6]

Contrario a lo que se cree, el contenido de la RAM no se pierde en cuanto la energía de la maquina deja de ser suministrada, si no que se desvanece gradualmente con el tiempo. Las temperaturas bajas reducen aún más el desvanecimiento de los bits en la RAM. Este efecto se conoce como efecto de remanencia [5]. Esto provoca que el contenido se pueda restaurar durante un cierto tiempo, lo que le da al atacante tiempo suficiente para desconectar, mover y volver a conectar las DRAM robadas a los sistemas del atacante. [6]

El primer artículo que se escribió de sobre este ataque fue de estudiantes de Princeton University de Halderman et al [2]. Ellos aprovechan el efecto de remanencia de DRAM para recuperar claves criptográficas almacenadas en la memoria. Esto con los modelos SDRAM, DDR1 y DDR2

El más rápido exhibe una pérdida completa de datos en aproximadamente 2,5 segundos (DDR2) y el más lento toma un promedio de 35 segundos (SDRAM). Sin embargo, todas las curvas de decaimiento muestran una forma similar, con un período inicial de decaimiento lento, seguido de un período intermedio de decaimiento rápido y luego un período final de decaimiento lento [2].

Halderman et al [2] cargaron un mapa de bits en la memoria y cortaron la energía para comprobar la remanencia de una de sus máquinas de prueba.

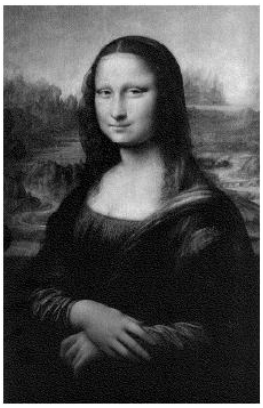

Fig 1. Imagen después de 5 seg

Como podemos notar la imagen es casi igual a la original por lo que no se han perdido muchos bits.

Gradualmente la figura se va desvaneciendo, lo podemos ver en las siguientes tres imágenes.

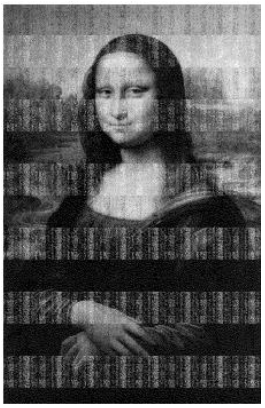

Fig 2. Imagen después de 30 [s]

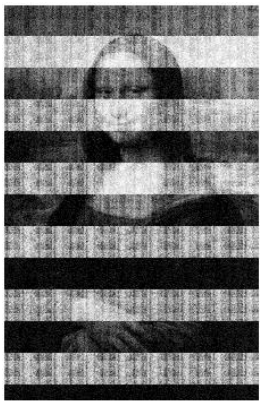

Fig 3. Imagen después de 60 [s]

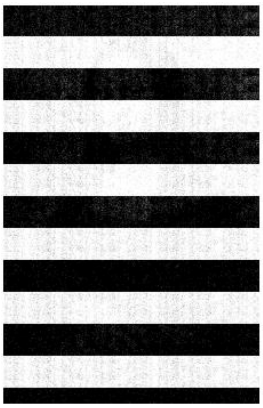

Fig 4. Imagen después de 5 [min]

La secuencia de imágenes anteriores es como la RAM sigue teniendo información y se desvanece gradualmente con un tiempo de segundos a minutos esto de forma relativamente rápido, pero la velocidad depende de cada memoria, aun así, si nosotros antes de apagar nuestro equipo enfriamos el modelo de DRAM a -50° C podemos ampliar ese tiempo [9]

Esto lo comentado anteriormente se puede apreciar en video titulado "*Lest We Remember: Cold Boot Attacks on Encryption Keys*" en el minuto 2:18

B. Implementación del ataque

Halderman et al [2] proponen 3 formas de llevar a cabo este ataque, la remanencia en estos métodos nos permite adquirir imágenes de memoria de las que se pueden extraer claves y otros datos sensibles. Lo anterior lo presenta del método más sencillo al más complejo y fuerte.

El primero utiliza el arranque en caliente, un procedimiento de reinicio de los sistemas operativos, en el sistema informático de la víctima. Para realizar un procedimiento de volcado de memoria, el atacante puede usar USB o arranque de red.[6]

Un ataque más avanzado corta brevemente la energía de la máquina, luego la restaura y arranca un kernel personalizado; esto priva al sistema operativo de cualquier oportunidad de limpiar la memoria antes de apagarse.[2]

Un ataque aún más fuerte corta la energía y luego trasplanta los módulos DRAM a una segunda PC preparada por el atacante, que extrae su estado. Además, este ataque priva al BIOS original y al hardware de la PC de cualquier posibilidad de borrar la memoria en el arranque [2] Para minimizar la pérdida de datos durante la transferencia del módulo, este método utiliza aire comprimido o nitrógeno líquido para congelar el módulo DRAM [6]

En la investigación de Halderman et al [2] se hicieron pruebas con SDRAM, DDR, DDR2 y descubrieron que las maquinas que usan memorias con tecnología más reciente tienden a resguardar la información por menos tiempo que las que utilizan memorias con tecnologías, aun con tiempos más cortos no se logra que sean inmunes a los ataques que plantearon [2]

C. Defensa contra el ataque

Halderman et al. Sugiere tres métodos de defensa conforme a los planteados en la sección anterior:

La defensa en contra del primer método es actualizar el sistema operativo para borrar el contenido de la memoria antes del arranque en caliente[3] [6]

3. un arranque en caliente es el proceso de reiniciar un ordenador o equipo de red sin apagarlo previamente [14]

La defensa contra el segundo método es configurar el BIOS para eliminar el contenido en el momento del arranque. Este método puede ser neutralizado por el método de ataque para restablecer la contraseña del BIOS descargando la batería CMOS [6]

El tercer método separa físicamente el módulo DRAM del sistema repentinamente, por lo que no le da al sistema operativo ni al BIOS la oportunidad de eliminar el contenido. Por lo tanto, este tercer método de ataque es el más difícil de defender. [6]

En este Halderman et al. propone soldar el módulo DRAM como defensa, pero Hoseok et al. argumenta que este método de defensa evita que los usuarios actualicen el módulo DRAM según sea necesario.

REFERENCIAS

[1] Armen Boursalian, & Mark Stamp. (2019). *BootBandit: A macOS bootloader attack*. Engineering Reports, 1(1). https://doi.org/10.1002/eng2.12032

[2] Center for Information Technology Policy. (2020, 14 octubre). *Lest We Remember: Cold Boot Attacks on Encryption Keys*. Recuperado 23 de marzo de 2022, de https://citp.princeton.edu/our-work/memory/

[3] C. Tan, L. Zhang and L. Bao, *"A Deep Exploration of BitLocker Encryption and Security Analysis,"* 2020 IEEE 20th International Conference on Communication Technology (ICCT), 2020, pp. 1070-1074, doi: 10.1109/ICCT50939.2020.9295908.

[4] González, A. (2021, 14 abril*). Aprende a encriptar un disco duro o una memoria externa. Ayuda Ley Protección Datos*. Recuperado 22 de marzo de 2022, de https://ayudaleyprotecciondatos.es/2020/06/09/encriptar-disco-duro/#:%7E:text=El%20cifrado%20del%20disco%20duro,en%20un%20disco%20duro%20cifrado.

[5] *Gruhn, M., & Muller, T. (2013). On the Practicability of Cold Boot Attacks. 2013 International Conference on Availability, Reliability and Security, Availability, Reliability and Security (ARES),* 2013 Eighth International Conference on, Availability, Reliability and Security (ARES), 2012 Seventh International Conference On, 390–397. https://doi-org.pbidi.unam.mx:2443/10.1109/ARES.2013.52

[6] H. Seol, M. Kim, T. Kim, Y. Kim and L. -S. Kim, *"Amnesiac DRAM: A Proactive Defense Mechanism Against Cold Boot Attacks,"* in IEEE Transactions on Computers, vol. 70, no. 4, pp. 539-551, 1 April 2021, doi: 10.1109/TC.2019.2946365.

[7] Online, T. H. P. (2021, 15 diciembre). *¿Qué es la memoria dinámica de acceso aleatorio (DRAM)?* Tienda HP México. Recuperado 24 de marzo de 2022, de https://www.hp.com/mx-es/shop/tech-takes/que-es-

[8] Offline Attack - Glossary | CSRC. (s. f.). CENTRO DE RECURSOS DE SEGURIDAD INFORMÁTICA. Recuperado 26 de marzo de 2022, de https://csrc.nist.gov/glossary/term/offline_attack dram#:%7E:text=DRAM%20significa%20%22memoria%20din%C3%A1mica%20de,los%20a%C3%B1os%2070%20%5B2%5D.

[9] P. (2008b, febrero 21). *Lest We Remember: Cold Boot Attacks on Encryption Keys* [Vídeo]. YouTube. https://www.youtube.com/watch?v=JDaicPIgn9U&feature=youtu.be

[10] Seguridad informática hacking ético : conocer el ataque para una mejor defensa (4a edición). (2018). Ediciones ENI.

[11] tok.wiki. (s. f.). *Ataque de arranque en frío Detalles técnicos y Usos*. hmong. Recuperado 23 de marzo de 2022, de https://hmong.es/wiki/Cold_boot_attack

[12] Yitbarek, S. F., Aga, M. T., Das, R., & Austin, T. (2017). *Cold Boot Attacks are Still Hot: Security Analysis of Memory Scramblers in Modern Processors*. https://doi-org.pbidi.unam.mx:2443/10.1109/HPCA.2017.10

[13] W. (2018, 13 septiembre*). The Chilling Reality of Cold Boot Attacks*. YouTube. Recuperado 23 de marzo de 2022, de 1https://www.youtube.com/watch?v=E6gzVVjW4yY&feature=youtu.be

[14] B. (2020d, julio 10). *¿Qué es un Arranque en Caliente?* Ordenadores y PortÃ¡tiles. Recuperado 29 de marzo de 2022, de https://www.ordenadores-y-portatiles.com/arranque-en-caliente/