TÉCNICAS DE REINICIO EN FRÍO: INFLUENCIA EN LA PRÁCTICA DE DILIGENCIAS DE ENTRADA Y REGISTRO

Joaquín Anguas Balsera

Perito Ingeniero en Informática

joaquim@anguas.com Telf. Móvil: 676 23 42 84

Ingeniero en Informática por la Facultat d'Informàtica de Barcelona, Universitat Politècnica de Catalunya, 1999. Máster en Ingeniería del Software por la Fundació Politècnica de Catalunya, Universitat Politècnica de Catalunya, 2006. Auditor de Sistemas de Información. Perito Ingeniero en Informática desde 2003.

Palabras Clave:

metodología forense, diligencia de entrada y registro, encriptación de discos, reinicio en frío

ABSTRACT

Las tecnologías de encriptación de discos representan un obstáculo para el análisis forense, impidiendo, a priori, la obtención de evidencias digitales a falta de las claves criptográficas.

Las técnicas de reinicio en frío nacen orientadas a la obtención de las claves criptográficas de disco de la memoria, liberando la prueba, si se dan las circunstancias adecuadas, de la voluntad del administrador del sistema de facilitar dichas claves de encriptación. Se fundamentan en la persistencia de la memoria de tecnología DRAM, que mantiene sus valores durante segundos e incluso minutos después de desconectar el equipo de la corriente. Esto permite el reinicio en un sistema operativo de pequeño tamaño que vuelque el contenido original de la memoria a un medio de almacenamiento externo.

Aunque como ya se ha dicho el propósito original de estas técnicas es analizar la memoria en busca de claves criptográficas, sus implicaciones son notablemente más amplias.

Tradicionalmente se ha preferido el análisis forense en frío, cortando el suministro eléctrico de los ordenadores objeto de captura para evitar que cualquier evento interno o externo pudiera destruir evidencias digitales. Pero dada la imposibilidad de realizar ciertos análisis de otra forma, y a pesar de las complicaciones e interrogantes que abre, el análisis de sistemas en caliente se ha hecho cada vez más común.

Las técnicas de reinicio en frío pondrían a disposición del ingeniero forense que ha de realizar el análisis el universo de evidencias memoria/disco completo, permitiendo análisis forenses que eran imposibles anteriormente.

Esta ponencia pone en contexto, estudia la diferente casuística y propone un conjunto de medidas para la correcta ejecución de una diligencia de entrada y registro con captura de memoria usando técnicas de reinicio en frío.

1 Introducción

Las diligencias de entrada y registro en particular y cualquier tipo de captura forense de datos en general, se encuentran en la raíz de la prueba: cualquier contaminación en origen la comprometerá en el futuro. Mientras que una captura forense puede realizarse sobre sistemas sobre los que se tiene control, las diligencias de entrada y registro se realizan sobre sistemas de terceros. Durante la ejecución de una diligencia de entrada y registro, cualquier complicación innecesaria es una fuente de error, por lo que los procedimientos deben ser simples, homogéneos y claros.

Durante años la aproximación al análisis forense de datos se basó en la captura del contenido del disco duro del ordenador objeto del análisis (análisis forense de datos en frío). Con el tiempo los escenarios de prueba se hicieron más complicados y se hizo necesario considerar el contenido de la memoria volátil, con la consiguiente proliferación de programas y dispositivos para su captura y análisis (análisis de datos en caliente). Con el advenimiento de los sistemas de encriptación de disco la situación se hizo más complicada, ya que en este caso el análisis en frío era poco menos que inútil: una copia de una unidad física encriptada es imposible de analizar ya que es el nivel lógico el que traduce el contenido del disco en algo legible.

Algunas herramientas de análisis en caliente acabaron dando soporte al acceso a nivel lógico a discos encriptados, pero en cualquier caso se hacía necesaria la colaboración de los administradores del sistema para facilitar el acceso lógico a los mismos.

Aunque existen mecanismos legales para forzar la entrega de claves criptográficas de discos, una persona que guarda información relevante en un soporte encriptado objeto de una diligencia de entrada y registro y no revela la clave, compromete la efectividad de la medida ordenada por el juez.

Halderman et al. (Halderman 2008) aprovechan la capacidad de la memoria DRAM para mantener su estado durante un tiempo después de suprimir el suministro de corriente a los módulos de memoria para tratar de identificar información que los sistemas operativos mantienen latente en memoria y que no sería accesible de otro modo.

Su aproximación influye en el planteamiento actual de las diligencias de entrada y registro y la captación forense de datos, ya que permite capturar e incorporar a la prueba el contenido de la memoria volátil de forma similar a la captura de disco.

2 Enfoques

Se podrían considerar tres enfoques a la hora de plantear un análisis forense de datos según el método de obtención: en frío, en caliente y con reinicio en frío.

2.1 Análisis forense en frío

Durante años ha sido práctica habitual, en la captura forense en general y en las diligencias de entrada y registro en particular, cortar la corriente de los ordenadores objeto de análisis y proceder a la copia bit a bit de los discos que contengan (SWGDE 2006).

De esta manera se pretendía evitar que se produjese algún evento que pudiera comprometer la actuación y evitar, así mismo, perjudicar en más de lo estrictamente necesario a quien asume

la medida. El ingeniero realiza posteriormente el análisis forense que considera oportuno a partir de una copia exacta de la copia bit a bit obtenida en la diligencia.

En este acercamiento al análisis forense se consideran los discos duros como elementos que tras la copia resulta explícitos y completos para el ingeniero que realiza el análisis posterior. A pesar de que cuando el sistema está en marcha los elementos de memoria volátil forman parte del universo de la prueba, bajo este enfoque prima la minoración de riesgos (reales o no) tanto en la ejecución de la medida como en el posible compromiso de la irreprochabilidad de la prueba. En determinadas circunstancias, como puede ser un sistema hibernado, es posible conseguir una imagen de la memoria en forma de fichero de hibernación, aunque la misma acción de hibernación podría haber permitido que se ejecuten procedimientos que podrían haber alterado el volcado de memoria o que al menos caen fuera del control del ingeniero forense.

Este enfoque es insuficiente en un escenario con tecnologías de encriptación de discos y en aquellos casos en los que se hace necesario el análisis de los datos en memoria cuando el sistema está en ejecución.

2.2 Análisis de datos en caliente

Impelidos por la necesidad de realizar análisis forenses que son imposibles en frío, se ha ido generalizando el análisis de datos en caliente. Tal y como describe Casey et al. (Casey 2008) dichas técnicas se han popularizado, existiendo diferentes herramientas comerciales que se enfocan a este tipo de actuaciones y un creciente mercado al respecto.

Hasta la aparición de las técnicas descritas en Halderman et al. (Halderman 2008) el análisis de datos en caliente era la única manera de evitar los efectos de las tecnologías de encriptación de discos, permitiendo acceso a las unidades desde el nivel lógico.

Aunque como bien expone Casey et al. (Casey 2008) el hecho de modificar el entorno de ejecución del sistema mientras está funcionando es algo que no tiene que representar ningún problema si se documenta adecuadamente y se preserva el estado de la prueba que se desea extraer, sí que es cierto que puede dejar más puertas abiertas a la posible impugnación de la misma.

2.3 Volcado de memoria obtenido usando técnicas de reinicio en frío

Que la tecnología de memoria DRAM no pierde su contenido inmediatamente tras cortar el suministro de corriente a los módulos de memoria es algo que se conocía desde los años 70. Pero según parece la comunicación de Halderman et al. (Halderman 2008) es la primera en medir los diferentes factores que influyen en este hecho y en ponerlo en su debido contexto.

En referencia a los temas relacionados con la captación y análisis forense de datos, el trabajo de Halderman et al. (Halderman 2008) haría tres aportaciones principales:

- Pone de manifiesto y cuantifica el deterioro de la memoria en función de la temperatura y el tiempo tras cortar el suministro de corriente a los módulos de memoria. A este respecto propone el uso de espráis quita-polvo para generar sobre los módulos temperaturas de hasta -50º.
- Describe la tecnología y el proceso para copiar el contenido de la memoria a un medio de almacenamiento externo, ofreciendo un rendimiento aproximado de 1Gb por minuto. Muestra sus resultados en referencia a aquellos elementos que pueden

comprometer la viabilidad de dicha copia, como pueden ser las memorias ECC, que son borradas al iniciarse el sistema o los sistemas de comprobación de memoria de BIOS que tienen un efecto similar.

- Muestra como de ese volcado de memoria se pueden extraer contraseñas, claves RSA y claves de encriptación y cómo utilizar estas últimas para desencriptar un disco duro encriptado usando tecnologías de encriptación de disco embebidas en diferentes sistemas operativos.

El procedimiento descrito de copia de la memoria a un medio de almacenamiento externo copia exactamente el contenido de la misma. Si bien es cierto que al arrancar el sistema una parte del BIOS se copia a memoria principal y el mismo sistema de arranque y copia que se usa para este fin reside en esta memoria y se copia en el proceso, con los tamaños de memoria actuales, aunque la huella relativa de ambos comparada con dicho tamaño es muy pequeña, por lo que la posibilidad de que se reescriban datos relevantes es también pequeña. Ambas cosas, BIOS y sistema de copia pueden ser además conocidas y adjuntadas a la copia para que sean tomadas en consideración por el ingeniero que ha de realizar el análisis forense de datos posterior.

La tercera aportación es relevante en relación a la etapa de análisis forense pero no para la de captación forense de datos. El trabajo de Halderman et al. (Halderman 2008) está orientado precisamente a este tercer objetivo y se plantea y ha sido considerado en general como el descubrimiento de una vulnerabilidad de los sistemas de encriptación de disco.

En el enlace http://citp.princeton.edu/memory/ puede encontrarse tanto documentación como herramientas para reproducir los resultados del trabajo.

3 Casuística y recomendaciones

Aunque en ocasiones es posible conocer a priori características detalladas de los sistemas objeto de la actuación, en general éstas son desconocidas, por lo que la diligencia debe ser diseñada de forma que se pueda dar una respuesta óptima al mayor porcentaje posible de situaciones.

En concreto lo que se propone es orientar el planteamiento de Halderman et al. (Halderman 2008) para la captura forense de la memoria volátil, adaptándolo a la casuística más común en una diligencia de entrada y registro.

Debe tenerse en cuenta que este tipo de procedimientos son susceptibles de provocar daños irreparables en los sistemas objeto de la diligencia y que deben realizarse por personal especializado y entrenado en su práctica.

Aunque la propuesta de Halderman et al. (Halderman 2008) se orienta hacia el arranque desde USB o red, quizás sería más recomendable por ser más común y fácil de configurar el inicio del sistema desde CD-ROM.

El caso ideal y el que debería ser más común sería un sistema con memoria no ECC, con una unidad lectora CD-ROM con capacidad de arrancar y un puerto USB libre.

El procedimiento para este caso sería muy simple: acceder a los módulos de memoria y enfriarlos mediante gas licuado, desconectar la corriente y volver a arrancar inmediatamente, configurar el BIOS para arrancar de CD-ROM y realizar la copia de la memoria a un medio USB extraíble.

Las siguientes circunstancias se apartarían de este caso ideal y deben tenerse en cuenta para minimizar el riesgo de fracaso de la actuación.

3.1 Arranque y copia

Ha de ser posible arrancar de red, USB o CD-ROM y ha de ser posible copiar a un dispositivo USB o en red. Si no es así y la situación lo requiere, existen alternativas que pasarían por mover la memoria previamente enfriada a un ordenador preparado a tal efecto o incluso modificar el sistema de arranque y copia para que residiese en un disco duro que se conectaría temporalmente como disco duro principal del ordenador a analizar.

3.2 Tipo de memoria

Si la memoria es ECC y dado que los BIOS de este tipo de sistema precisan reiniciar toda la memoria para su correcto funcionamiento, es preciso enfriar y extraer la memoria para montarla en otro ordenador que soporte el mismo tipo de memoria pero no implemente ECC.

Debe tenerse en cuenta que aunque en general las tecnologías de memoria mantienen compatibilidad respecto a diferencias de velocidad, no es así entre tecnologías (obviamente el número de espigas es diferente) o voltajes.

3.3 Bios bloqueado por contraseña

Es necesario habilitar el arranque desde CD-ROM, USB o red y desactivar la comprobación inicial de memoria del sistema, por lo que debería ser posible entrar y modificar los valores del BIOS. Si el BIOS está protegido por contraseña, se debe intentar su reinicio. Como alternativa al arranque desde CD-ROM, USB o red, podría usarse un disco duro configurado con el sistema de arranque y copia.

3.4 Modificación del sistema a analizar

En casos extremos debería ser posible modificar los componentes que fuera necesario del sistema objeto de análisis (por ejemplo añadir un CD-ROM si no tuviese o cambiar temporalmente el disco de arranque por otro con el sistema de arranque y copia de la memoria). Debe tenerse en cuenta que las modificaciones no pueden alterar en ningún modo la información en discos o memoria, que se debe documentar cada cambio detalladamente y que es necesario tener todo lo necesario preparado antes de enfriar los chips y cortar la corriente.

3.5 Casos que no se cubren

En el caso de que:

- El ordenador use memoria ECC ó
- No sea posible arrancar desde un medio con el sistema de arranque y copia ó
- No sea posible disponer de un dispositivo de almacenamiento externo donde copiar el volcado

Si no se dispone de otro ordenador que permita lo anterior y que acepte el tipo y cantidad de memoria necesario, no será posible realizar la captación de datos.

3.6 Material

Es necesario:

- Sistema de arranque y copia en CD-ROM, USB o red arrancable
- Disco duro externo de gran tamaño para recibir las copias tanto de la memoria como de los discos duros
- Espray de gas comprimido del usado para eliminar polvo de dispositivos electrónicos (duster)
- Ordenador con conexión a internet para consultar manuales, etc
- Idealmente un ordenador portátil y uno de sobremesa que no sean de última generación, con memoria no ECC, configurados para arrancar de CD-ROM y con el sistema de comprobación de memoria deshabilitado

3.7 Preparación y test

Deben prepararse todas las herramientas y material necesario para la prueba, habiéndose probado su efectividad en laboratorio y se deben simular actuaciones que se salgan del caso ideal. Aquellos que han de participar en la actuación deben haber experimentado con las herramientas y procedimientos por ellos mismos.

3.8 Ejemplo de procedimiento

Con objeto de dotar de contexto a las consideraciones anteriores, se propone un ejemplo de procedimiento en el que se puede ver la importancia real de las diferencias posibles respecto a la situación ideal.

Como previo:

- Se debe documentar cada paso de la actuación.
- El sistema objeto de análisis debe estar en funcionamiento.
- Dependiendo del objeto de la diligencia, el ordenador se debe desconectar de la red.
- Se debe impedir en todo momento que nadie tenga acceso físico al sistema objeto de la diligencia.
- En caso de urgencia justificada debe ser posible obviar pasos del procedimiento, entendiendo las consecuencias que esto puede conllevar.

Pasos:

- Realizar una inspección ocular del sistema, buscar marca, modelo y número de serie.
- Si no tiene lector de CD-ROM mirar si dispone de puertos USB y cuantos.
- Buscar en internet características de memoria (número de espigas, tecnología y voltaje) a partir del modelo, así como su distribución en el ordenador, manuales de servicio para acceso a la memoria, si es posible buscar menús del BIOS y localizar configuración de inicio y USB, así como procedimiento de reinicio de contraseña si lo hay.
- Acceder a la memoria según los manuales de servicio y anotar el tipo y cantidad de memoria del sistema.
- Si el tipo de memoria es ECC o no tiene ni CD-ROM ni USB o el BIOS está protegido por contraseña o no permite arrancar de red, CD-ROM o USB, comprobar si es posible instalar el tipo y cantidad de memoria del sistema en alguno de los ordenadores disponibles a tal efecto.

- Si efectivamente se dispone de un ordenador adecuado, rociar la memoria con el gas invirtiendo el bote al efecto de que se licue el gas y enfríe los chips, desenchufar el ordenador y quitar la batería si es un portátil, poner la memoria en el otro ordenador respetando el orden de bancos, colocar el CD-ROM de inicio y el disco duro externo y encenderlo, una vez arrancado, realizar la copia de la memoria.
- En caso de no ser necesario el ordenador alternativo, proceder de forma similar con el sistema objeto de análisis, es decir, rociar la memoria con el espray de gas con la válvula hacia abajo de manera que enfríe los chips, desenchufar el ordenador y quitar la batería si es un portátil, poner la memoria en el otro ordenador respetando el orden de bancos, colocar el CD-ROM de inicio y el disco duro externo y encenderlo. Inmediatamente entrar en el BIOS, comprobar que se encuentra deshabilitada la comprobación de memoria (Quickboot activado) y el arranque desde CD-ROM. Guardar los valores del BIOS y reiniciar, cuando se haya completado el arranque, realizar la copia de la memoria.
- Llevar a cabo el resto de la actuación.

4 Contramedidas y posible evolución

El revuelo que ha generado la publicación de Halderman et al. (Halderman 2008) ha atraído múltiples comentarios acerca de cómo evitar el éxito de la práctica descrita, ya que no se debe olvidar que los autores la plantean como una vulnerabilidad.

La mayoría de las propuestas se basan en sistemas para mantener las claves criptográficas a salvo, mientras que sólo unas pocas, con mayor o menor fortuna se enfocan a evitar la captación del contenido de la memoria.

En este último caso se proponen principalmente medidas que deben ser implementadas por los fabricantes, como modificar los sistemas de arranque o desconexión para que borren efectivamente la memoria o el uso de TPM en los sistemas de memoria.

En cuanto a fórmulas que un usuario puede implementar por si mismo podríamos citar la utilización de memoria ECC y la fijación permanente de la misma a los slots.

La industria buscará mejorar los productos y evitar que se puedan realizar acciones como las descritas en aras de privacidad y la seguridad. Si esas mejoras se usan para fines legítimos o no, está naturalmente por encima de lo que la industria puede controlar.

5 Conclusiones

La publicación de Halderman et al. (Halderman 2008) aunque orientada a la obtención de claves criptográficas, inspira nuevas formas de enfrentarse a la captura forense de datos y al análisis forense en general.

En este documento se ha puesto en contexto dicha publicación, se han visto las implicaciones que tiene en la captura y análisis forense de datos, se ha estudiado la casuística asociada a un acercamiento similar en la práctica de una diligencia de entrada y registro y se han dado recomendaciones al respecto.

6 Referencias

Casey, Eoghan; Stellatos, Gerasimos J. (2008). "The impact of full disk encryption on digital forensics". *Operating Systems Review* 42 (3): 93–98.

J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten (2008). "Lest We Remember: Cold Boot Attacks on Encryption Keys" *Proc. 2008 USENIX Security Symposium*: 45-60. http://citp.princeton.edu/memory/

SWGDE (2008). "SWGDE Best Practices for Computer Forensics Version 2.1 (July 2006)" http://www.swgde.org/documents/swgde2006/Best_Practices_for_Computer_Forensics%20July06.pdf