Métodos de Limpieza (Degaussing y Gutmann)

Ibañez Mamani Richard Alejandro
Universidad Mayor De San Andrés
Carrera De Informática
Simulación de Sistemas
axl.ale.ar@hotmail.com

RESUMEN

Hasta el momento, se ha hablado de métodos de limpieza o borrado de discos duros u otros dispositivos magnéticos siendo ya una necesidad destruir información sin dejar rastro alguno. En este artículo, se describen las prácticas adecuadas para la eliminación de información. En este documento informativo, específicamente se mostrarán en que consisten el Método de Degaussing y el método de Gutmann, observandose hasta que grado puede darnos la solución de "limpieza" para nuestro disco duro.

Palabras clave

Métodos, limpieza o borrado, Degaussing, Gutmann.

1. INTRODUCCIÓN

Borrar de manera definitiva los datos en un medio magnético tiene toda una problemática asociada.

Sin embargo, y dependiendo del medio usado (unidades de disco, cintas, diskettes, etc.), el proceso de eliminación total de los datos se ve afectado por diversos factores.

El Departamento de Defensa de los Estados Unidos cuenta con toda una serie de recomendaciones sobre cómo "sanitizar" un medio magnético, esto es, el proceso por el cual la información clasificada es removida por completo, en donde ni siquiera un procedimiento de laboratorio con las técnicas conocidas a la fecha o un análisis pueda recuperar la información que antes estaba grabada. Aunque en un comienzo los procedimientos a seguir pueden parecer algo paranoicos, la (relativa) facilidad con la que se puede recuperar información que se creía borrada hace necesario tomar medidas extremas a la hora de eliminar datos confidenciales o comprometedores. En enero de 1995, esta entidad publicó un documento, el "National Industrial Security Program Operating Manual" (NISPOM), más comúnmente referenciado como "DoD 5220.22-M" , que detalla toda una serie de procedimientos de seguridad industrial, entre ellos, cómo eliminar datos contenidos en diferentes medios.

A partir de los lineamientos presentes en 5220.22-M , otro organismo estadounidense, el Defense Scurity Service, publicó una "Matriz de Sanitización y Borrado" (Degaussing), que explica de manera práctica los pasos a seguir para remover por completo información sensitiva, y un algoritmo ya conocido de borrado o limpieza como es el método Gutmann.

2. METODO DEGAUSSING

2.1 Explicación

La Matriz de Limpieza y Sanitización es una acumulación De métodos conocidos y aprobados para limpiar y/o sanitizar diversos medios y equipo. Cuando NISPOM fue publicado, el Rango Extendido Tipo II, Tipo III y los degaussers de Propósito Especial no existían. Esto resultaba en la necesidad de destruir todos los medios con un factor de coercividad, mayor a 750 oersteds (unidad que mide la fuerza magnetizante necesaria para producir una fuerza magnética deseada a lo largo de una superficie) y la mayoría de discos magnéticos cuando ya no fueran necesarios como soporte para una misión clasificada. Ahora, la "National Security Agency" norteamericana (NSA) ha evaluado degaussers de cinta magnética que satisfacen los requerimientos del gobierno para sanitizar cintas magnéticas de hasta 1700 oersteds.

Las cintas magnéticas se encuentran divididas en Tipos. La cinta magnética de Tipo I tiene un factor de coercividad que no excede los 350 oersteds y puede ser usada para sanitizar (degauss) todos los medios de Tipo I. La cinta magnética de Tipo II tiene un factor de coercividad entre 350 y 750 oersteds y puede ser usada para sanitizar todos los medios Tipo I y II. La cinta magnética Tipo II de Rango Extendido tiene un factor de coercividad entre 750 y 900 oersteds y puede ser usada para sanitizar todos los medios Tipo I, Tipo II y Rango Extendido. Finalmente, las cintas magnéticas Tipo III, comúnmente conocidas como cintas de alta energía (por ejemplo, cintas de 4 ó 8mm), tienen un factor de coercividad actualmente identificado como entre 750 y 700 oersteds y puede ser usada para sanitizar todos los tipos de cintas magnéticas.

Para sanitizar (degauss) todos los medios de disco, rígidos o flexibles (por ej., diskettes, Bernoulli, Syquest y unidades de Disco Duro) se deben usar degaussers de Unidad de Disco. Para este tipo de dispositivos la NSA tiene una nueva categoría de degaussers, conocida como Degaussers de Propósito Especial. DSS, como todas las agencias del DoD, referencia el "Information Systems

Security Products and Services Catalog" como guía de anitización de memoria y medios. NSA publica el "Information Systems Security Products and Services Catalog" entre sus productos y servicios de seguridad para sistemas de

información. La lista de productos degausser (DPL) está dedicada a los degaussers de discos y cintas magnéticas. La DPL hace un excelente trabajo identificando los fabricantes de degaussers y los diferentes tipos de éstos.

1.2. Descripción del Método Degaussing

a. Degauss con un degausser Tipo I, II o III.

b. Degauss con el mismo Tipo (I, II o III) de degausser.

c. Sobreescriba todos los lugares direccionables con un sólo carácter.

d. ESTE MÉTODO NO ES APROBADO PARA SANITIZAR MEDIOS QUE CONTENGAN INFORMACIÓN TOP SECRET.

Antes de adquirir un producto de sanitización, se deben analizar cuidadosamente los costos totales asociados con la sobre escritura/sanitización. Dependiendo del ambiente del contratador, el tamaño del driver y las diferencias en los tiempos individuales de los productos sobre los que se va a efectuar la sanitización, podría ser que la destrucción de los medios fuera la elección más económica como método de sanitización.

Sobrescribir todas las locaciones direccionables con un carácter, luego con su complemento. Verificar que el carácter "complemento" fue escrito exitosamente en todas las locaciones direccionables, después sobrescribir todas las locaciones direccionables con caracteres aleatorios; verificar la tercera sobreescritura. La utilidad de la sobreescritura debe escribir/leer para "crecer" las listas/sectores defectuosos o el disco debe estar mapeado antes del uso clasificado inicial y re-mapeado antes de la sanitización. La diferencia en la comparación de listas debe ser discutida con el Representante de Seguridad Industrial de DSS (IS Rep) y/o Information System Security Professional (ISSP) antes de la desclasificación. Es necesario notar que las utilidades de sobreescritura deben estar autorizadas por DSS antes de ser usadas.

e. Sobrescriba todas las locaciones direccionables con un carácter, su complemento y luego un carácter aleatorio.

f. Cada sobreescritura debe residir en memoria por un periodo mayor al que residieron los datos clasificados.

g. Sobreescriba todas las locaciones con un patrón aleatorio, después con ceros binarios y finalmente con unos binarios.

h. Remueva todas las fuentes de poder, incluyendo el poder de la batería.

i. Realice un borrado de chip completo de acuerdo a las especificaciones del fabricante.

j. Efectúe i, luego c un total de tres veces.

k. Efectúe un borrado ultravioleta de acuerdo con las recomendaciones del fabricante.

l. Haga k, pero incremente el tiempo por un factor de tres.

m. Destrucción. Ver 1) y 2) más abajo.

n. Destrucción requerida sólo si se contiene información clasificada.

o. Correr una página (podría ser la prueba de tipos de letra) cuando el ciclo de impresión no fue completado (por Ej., si el papel se atoró o hubo una falla eléctrica). Eliminar la salida como no-clasificada si un examen visual no revela ninguna información clasificada.

p. Las cintas deben ser destruidas y los rodillos deben ser limpiados.

q. Inspeccione y/o pruebe la superficie de la pantalla buscando evidencia de información "quemada" (burn-in). Si se encuentra, la pantalla debe ser destruida.

1) Todos los métodos de destrucción deben ser autorizados por el DSS antes de ser usados. Los posibles tipos de destrucción son:

Desintegrar, Incinerar, Pulverizar, Picar o Fundir.

2) NSA ofrece destruir medios AIS (Automated Information Systems) clasificados no relacionados con COMSEC (Communications Security), del gobierno o de contratantes. Contratantes que no sean del DoD deben obtener una carta

Tabla 1. Tipos de degausser y sus características

Medio	Limpieza					Sanitización														
Cinta Magnética																				
Tipo I	a					b								m						
Tipo II	a					b								m						
Tipo III	a					b								m						
Disco Magnético																				
Bernoullis	a	c				b								m						
Disco Flexible	a	c				b								m						
Disco Rigido no-removible		c				a		d						m						
Disco Rigido removible	a	c				a		d						m						
Disco Óptico																				
Read Many, Write Many		c												m						
Read Only														m	n					
Write Once, Read Many (Worm)														m	n					
Memoria																				
Dynamic Random Access Memory (DRAM)		c	h				c				h			m						
Electronically Alterable PROM (EAPROM)				i									j	m						
Electronically Erasable PROM (EEPROM)				i						g				m						
Erasable Programmable ROM (EPROM)					k		c						l	m					l luego c	
Flash EPROM (FEPROM)				i			c				i			m					c luego i	
Programmable ROM (PROM)		c												m						
Magnetic Bubble Memory		c				a	c							m						
Magnetic Core Memory		c				a			e					m						
Magnetic Plated Wire		c					c		f					m					c y f	
Magnetic Resistive Memory		c												m						
NonVolatile RAM (NOVRAM)		c	h				c				h			m						
Read Only Memory (ROM)														m						
Synchronous DRAM (SDRAM)		c	h				c				h			m						
Static Ryom Access Memory (SRAM)		c	h				c		f		h			m					c y f	
Equipos																		q		
Monitor			h																	
Impresora de Impacto			h								h						p		p luego h	
Impresora Láser			h								h					o			o luego h	

de su cliente autorizando a NSA para destruir su información clasificada o haber revisado los contratos de especificación de clasificación de seguridad (DD254).

3. METODO DE GUTMANN

El Método de Gutmann es un para seguro del contenido de la computadora de , por ejemplo . Ideado por y aplicada por Colin, han escrito una serie de 35 sobre la región que se borrará.

La selección de patrones asume que el usuario no sabe el mecanismo de codificación usado por la impulsión, y así que incluye los patrones diseñados específicamente para tres diversos tipos de impulsiones. Un usuario que sabe qué tipo de codificar las aplicaciones de la impulsión puede elegir solamente esos patrones pensó para su impulsión. Una impulsión con un diverso mecanismo de codificación necesitaría diversos patrones. La mayor parte de los patrones en el método de Gutmann fueron diseñados para los más viejos discos codificados /. Las impulsiones relativamente modernas ya no utilizan más las viejas técnicas de codificación, haciendo muchos de los patrones especificados por Gutmann "superfluos".

Por ejemplo:

Señal análoga:

Señal numérica ideal +11.1 -8.9 +9.1 -11.1 +10.9 -9.1: diferencia +10.0 -10.0 +10.0 -10.0 +10.0 -10.0: señal anterior +1.1 +1.1 -0.9 -1.1 +0.9 +0.9: +11 +11 -9 -11 +9 +9

Esto se puede entonces hacer otra vez para ver los datos anteriores escritos:

Señal recuperada:

+11 +11 -9 -11 +9

Señal numérica ideal +9: diferencia +10.0 +10.0 -10.0 -10.0 +10.0 +10.0: +1 +1 +1 -1 -1 -1

señal anterior: +10 +10 -10 -10 -10 -10

En 1996, cuando este método fue desarrollado, era posible utilizar un digital para recuperar ocho niveles de sobrescritura, sin dañar la impulsión. Densidades desde entonces más altas del disco tienen probablemente reducido el número de sobrescritura necesario para borrar totalmente datos.

Sin embargo, sobrescribir el disco con datos al azar no siempre trabajará en varias ocasiones. La de un medio cambia con la frecuencia del campo magnético. Esto significa que un campo de una frecuencia más baja penetrará más profundo en el material magnético en la impulsión que la de alta frecuencia. Una señal de baja frecuencia todavía será tan perceptible incluso después de que hayan sido centenares sobrescritos en ese momento por una señal de alta frecuencia.

Los patrones usados se diseñan para aplicar campos magnéticos

Tabla 2. Los 35 patrones del método de Gutmann

Paso	Datos escritos		Modele escrito al disco para el esquema de codificación apuntado		
	En Binario notación	En Tuerca hexagonal notación	(1,7) RLL	(2,7) RLL	MFM
1	(Al azar)	(Al azar)			
2	(Al azar)	(Al azar)			
3	(Al azar)	(Al azar)			
4	(Al azar)	(Al azar)			
5	01010101 01010101 01010101	55 55 55	100...		000 1000...
6	10101010 10101010 10101010	AA AA AA	00 100...		0 1000...
7	10010010 01001001 00100100	92 49 24		00 100000...	0 100...
8	01001001 00100100 10010010	49 24 92		0000 100000...	100 100...
9	00100100 10010010 01001001	24 92 49		100000...	00 100...
10	00000000 00000000 00000000	00 00 00	101000...	1000...	
11	00010001 00010001 00010001	11 11 11	0 100000...		
12	00100010 00100010 00100010	22 22 22	00000 100000...		
13	00110011 00110011 00110011	33 33 33	10...	1000000...	
14	01000100 01000100 01000100	44 44 44	000 100000...		
15	01010101 01010101 01010101	55 55 55	100...		000 1000...
16	01100110 01100110 01100110	66 66 66	0000 100000...	00000 10000000...	
17	01110111 01110111 01110111	77 77 77	100010...		
18	10001000 10001000 10001000	88 88 88	00 100000...		
19	10011001 10011001 10011001	99 99 99	0 100000...	00 10000000...	
20	10101010 10101010 10101010	AA AA AA	00 100...		0 1000...
21	10111011 10111011 10111011	BB BB BB	00 101000...		
22	11001100 11001100 11001100	CC CC CC	0 10...	0000 10000000...	
23	11011101 11011101 11011101	DD DE LA DD DE LA DD	0 101000...		
24	11101110 11101110 11101110	EE EE EE	0 100010...		
25	11111111 11111111 11111111	FF FF FF	0 100...	000 100000...	
26	10010010 01001001 00100100	92 49 24		00 100000...	0 100...
27	01001001 00100100 10010010	49 24 92		0000 100000...	100 100...
28	00100100 10010010 01001001	24 92 49		100000...	00 100...
29	01101101 10110110 11011011	DB de 6D B6		0 100...	
30	10110110 11011011 01101101	B6 DB 6D		100...	
31	11011011 01101101 10110110	DB 6D B6		00 100...	
32	(Al azar)	(Al azar)			
33	(Al azar)	(Al azar)			
34	(Al azar)	(Al azar)			
35	(Al azar)	(Al azar)			

que se alternan de varias frecuencias y de varias fases a la superficie de la impulsión y de tal modo para aproximar el material debajo de la superficie de la impulsión.

3.1. Los 35 patrones a seguir del método Gutmann

Cada uno de patrones fue diseñado con una específica para proyectados en mente, que cada patrón apunta. La impulsión se escribe para a todos los pasos aun cuando la tabla mencionada demuestra solamente las configuraciones de bits para los pasos que se apuntan específicamente en cada esquema de codificación. El resultado final debe obscurecer cualquier dato sobre la impulsión de modo que solamente la exploración física más avanzada (por ejemplo usar un) de la impulsión es probable poder recuperar cualquier dato.

La serie de patrones es como sigue:

6. CONCLUSIONES

Los métodos de Degaussing y Gutmann, son algunos de los tantos métodos utilizados para el borrado y limpieza de medios magnéticos, para así poder tener mayor seguridad en que nuestros archivos importantes ya borrados no podrán ser recuperados por ningún otro software, ya que si son archivos de suma importancia y confidencialidad atraerían un gran número de problemas al usuario o empresa que los perdió o no los elimino por completo, como en casos de entidades bancarias y empresas, si llegaran a personas ajenas a la entidad el daño podría ser muy fatal.

Con eso concluimos que estos métodos deben ser estudiados y practicados para todos los usuarios o clientes que manejen un gran número de información el cual puede ser perjudicial en manos de personas ajenas.

8. REFERENCIAS

[1] http://translate.roseville.ca.us/ma/enwiki/es/Data_remanence

[2] http://www.cdmatic.com/index.php/destacados/degausser-v91hd-dlt.htmlhttp://translate.roseville.ca.us/ma/enwiki/es/Degaussing/3#Degaussing_magnetic_data_storage_media

[3] http://www.forensics-intl.com/art12.html

[4] http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm

[5] http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm

[6] http://www.encase.com/html/how_encase_works.html

[7] http://www.forensics.com/products/welcome.html?peru.html