**Können Nachrichtendienste überschriebene Daten lesen?**

**Können Nachrichtendienste überschriebene Daten lesen? Eine Reaktion auf Gutmanns Papier.**(Übersetzung von Ch. Müller, ITRIS)

Behauptungen, dass Nachrichtendienste überschriebene Daten auf Laufwerken lesen können kursieren seit Jahren. Die am häufigsten zitierte Quelle ist ein Papier von Peter Gutmann, das bei einer Usenix Konferenz 1996 vorgestellt wurde. (*Secure Deletion of Data from Magnetic and Solid-State Memory*)

Ich fand das eine ausserordentliche Behauptung, die ausserordentliche Beweise verlangte. An einem Nachmittag in der Bibliothek der angewandten Wissenschaft an der Harvard-Schule hatte ich die Möglichkeit, das Papier und viele der Hinweise, die darin enthalten sind, zu überprüfen. (*http://www.usenix.org/publications/library/proceedings/sec96/full\_papers/gutmann/index.html*)

Selbstverständlich legen moderne Betriebssysteme Kopien von " gelöschten" Dateien in temporären Dateiverzeichnissen, nicht zugewiesenen Sektoren, Swap Files, korrigierten Bad Blocks, usw. ab. Aber Gutmann glaubt, dass ein überschriebener Sektor mit Hilfe eines hochentwickelten Mikroskops zurückgewonnen werden kann und diese Behauptung ist unkritisch von zahlreichen Leuten angenommen worden. Ich denke jedoch nicht, dass diese Personen die Referenzen in Gutmanns Papier nachverfolgt haben.

Gutmann erklärt, dass wenn ein "1" Bit über ein "0" Bit geschrieben wird, das tatsächliche Resultat näher an 0.95 ist und wenn eine eins mit eins überschrieben wird, näher an 1.05. Dies angenommen, zusammen mit einem Lesekopf der 20-mal so empfindlich ist wie in einem Serienlaufwerk und einem bekannten Datenmuster, das über die Daten geschrieben wurde, könne man die Unterdaten zurückgewinnen.

Die Hinweise, die Gutmann zur Verfügung stellt lassen sein Werk ziemlich übertrieben erscheinen. Kein Hinweis führt zu einem Beispiel, bei dem vertrauliche Daten wiederhergestellt wurden. Eher beziehen sie sich auf Experimente in denen STM-Mikroskopie verwendet wurde, um einzelne Bits zu überprüfen, und dabei wurden einige Reste der überschriebenen Daten gefunden.

Es gibt viel Literatur über Magnetkraft-Raster-Tunnel-Mikroskope (MFM = Magnetic Force Microscope oder STM = Scanning Tunneling Microscope) für Bits, die auf Magnetträger geschrieben werden. Der offensichtliche Punkt dieser Literatur ist nicht, überschriebene Daten zurückzuholen, sondern das Design der Lese-Schreibköpfe zu prüfen und zu verbessern. Zwei der Hinweise (Rugar , Gomez) enthielten Abbildungen der überschriebenen Bits und zeigten Teile der ursprünglichen Daten, die in den Mikrofotografien deutlich sichtbar sind. Diese wurden von den Autoren als Beispiele des sub-optimalen Kopfdesigns verwendet. Die Gesamtzahl den sichtbaren Bits war 6 in einem Foto und 8 im anderen. Keine der Mikrofotografien war ein Gesamterfolg, weil in einem Fall nur Übergänge von eins zu null sichtbar waren, und in der anderen einer der Übergänge nicht eindeutig erkennbar war. Dennoch nehme ich an, dass überschriebene Bits unter bestimmten Umständen wahrnehmbar sein könnten.

So kann ich sagen, dass Gutmann niemanden zitiert der behauptet die Unterdaten in überschriebenen Sektoren lesen zu können, noch zitiert er Artikel, die die üblichen Disk-Wipe Programme als völlig genügend erachten.

Ich sollte diesen letzten Punkt ein bisschen erklären. Ich war nicht imstande, eine Kopie der Hauptthese mit dem Titel "Detection of Digital Information from Erased Magnetic Disks" von Venugopal Veeravalli zu finden. Ein kurzer Besuch auf seiner Webseite zeigt, dass er nie etwas zu diesem Thema veröffentlicht hat, oder zu einem in Verbindung stehenden Thema. Sein Arbeitsgebiet ist Sicherheit in der Mobilkommunikation und seine anderen Arbeiten zeigen auch keine Vertrautheit mit STM-Mikroskopen. So bin ich ziemlich sicher, dass er keine Maschine entworfen hat um Unter-Daten mit einem "unwrite" Systembefehl zu lesen. In einer E-Mail-Nachricht sagte mir Dr. Veeravalli, dass seine Arbeit theoretisch war und er studierte die Möglichkeit der Anwendung von DC-Löschköpfen. Die Arbeit wurde inzwischen veröffentlicht. Sie ist in der Tat theoretisch, hat aber quantitative Vorhersagen über die Möglichkeit der Wiederherstellung von Daten mit verschiedenen Graden der Löschung. Es gibt darin keine Hinweise, dass gewöhnliche Löschverfahren unzulänglich sein könnten.

Gutmann behauptet, dass " Geheimdienste viel Sachkenntnis haben diese verwaschenen Bilder" auszuwerten, aber es gibt keinen Hinweis für diese Aussage. Es gibt 18 Hinweise im Papier, aber keiner von denen, die ich finden konnte, bezog sich auf diese Möglichkeit. Weitere Artikel von verschiedenen Autoren machen diesen Anspruch geltend, aber sie zitieren nur Gutmann, liefern also keinen zusätzlichen Beweis für seinen Anspruch.

Gutmann erwähnt, dass nach einer einfachen Einstellung der MFM Vorrichtung, die Bits innerhalb von Minuten fliessen. Dieses kann zutreffend sein, aber die Bits auf die er sich bezieht, sind nicht von den Plattendaten, sondern von den Pixeln der Abbildung der Plattenoberfläche. Charles Sobey hat ein informatives Papier geschrieben "Recovering Unrecoverable Data" mit ein paar quantitativen Informationen zu diesem Punkt. Er vermutet, dass er mehr als ein Jahr dauern würde, um eine einzelne Serverplatte mit neuer MFM Technologie zu scannen und zig Terabyte von Bilddaten verarbeitet werden müssten. In einem Abschnitt des Papiers schlägt Gutmann vor, Disks in 4 Durchläufen mit echten Zufallsdaten zu überschreiben. Dies weil er anscheinend annimmt, dass pseudo-zufällige Daten einem Ermittler bekannt sein könnten. Ein einzelnes Überschreiben ist jedoch genügend, wenn es wirklich zufällige Daten sind, selbst mit einem STM-Mikroskop mit weit besseren Leistungen als in den Referenzen beschrieben. Tatsächlich interferieren Daten, die zeitlich vor den gesuchten Daten geschrieben worden sind, mit diesen genauso wie die Daten die danach geschrieben werden. das STM Mikroskop kann dies nicht unterscheiden. Es ist nicht wie bei Tinte wo die neuere Schrift physikalisch über der alten liegt.

Nach der Veröffentlichung dieser Informationen in einer lokalen Email-Liste bekam ich eine Antwort mit dem Inhalt, dass es für die Wiederherstellung der überschriebenen Daten eine ganze Industrie gibt und dass eine Suche auf Google nach "recover overwritten data" einige Firmen hervorbringt, die diesen Service anbieten. In der Tat handelt es sich dabei um viele Unternehmen, aber alle ausser einem betonen ausdrücklich, dass sie " überschriebene *Dateien* wiederherstellen " können, was eine ganz andere Angelegenheit ist. Eine überschriebene Datei ist eine, deren Name überschrieben worden ist, aber nicht ihre Sektoren. Partitionierung, Formatierung und " Ghosting" beeinflussen gewöhnlich nur einen kleinen Teil der physikalischen Scheibe und lassen viel Potenzial zum Lesen von Sektoren, um versteckte Daten wieder zu finden. Es gibt keinen Hinweis im Marketing-Material, dass diese Unternehmen physikalisch überschriebene Sektoren lesen können. Die eine Ausnahme die ich fand war "Dataclinic" in Grossbritannien. Diese Firma reagierte nicht auf eine EMail Anfrage und sie erwähnen keine STM-Anlage auf ihrer Website.

Ein Brief von einem australischen Ermittler für Mordfälle bestätigt meine Ansicht, dass sogar Polizeibehörden keinen Zugang zur Technologie, wie sie Gutmann beschreibt, haben.

Selbstverständlich ist es einige Jahre her, seit Gutmann sein Papier veröffentlichte. Möglicherweise haben sich die Mikroskope verbessert? Ja…! Aber Datendichten sind auch höher geworden. Eine Stunde Suche im Internet hat bei allen Standorten mit STM Technologie keine Hinweise gebracht, dass eines dieser Labors in der Lage wäre überschriebene Daten zu lesen.

Vor kurzem wurde mir eine faszinierende Arbeit von Wright, Kleiman und Sundhar zugeschickt (2008) die tatsächliche Daten bezüglich der Genauigkeit der zurückgewonnenen Bilddaten enthält. Während die Bilder ein paar Informationen über überschriebene Bits beinhalten, ist die Fehlerhäufigkeit so hoch, dass es schwierig ist, sich die Tauglichkeit für die Praxis vorzustellen. Auch wenn ein paar zufällige Wörter aus Tausenden heraus zurückgewonnen werden konnten, würde die überwiegende Mehrheit der anscheinend wiederhergestellten Wörter falsch sein.

Eine andere Tatsache ist, dass es bisher niemandem gelungen ist, die "18 minute gap" (18 Minuten Lücke) zu lesen, die die Sektretärin Rosemary Woods auf dem Tonband von Nixon, den Watergate-Einbruch besprechend, unbeabsichtigt erzeugt hat. Trotz der Tatsache, dass die Datendichte auf einem analogen Recorder der Sechziger Jahre ungefähr eine Million mal niedriger ist als bei der gegenwärtigen Disk-Technologie und bei Audioaufnahmen nicht ein so hohes Mass an Genauigkeit nötig wäre, ist nicht eine einzige Silbe zurückgewonnen worden.

Die Forderung der militärischen Streitkräfte und der Nachrichtendienste, dass Laufwerke mit vertraulicher Information eher zerstört als gelöscht werden sollen, muss manchmal als Beweis herhalten, dass diese Dienste überschriebene Daten lesen können. Ich denke, dass die Wirklichkeit weit prosaischer ist. Der Techniker, der mit der Verschrottung eines Festplattenlaufwerks beauftragt wird, hat möglicherweise nicht genügend Computerwissen, um zu erkennen, ob der Befehl "urandom > /dev/sda2c1" die gesamte Platte, oder nur eine Partition mit zufälligen Daten beschrieben wird. Oder ob der Vorgang wirklich wie gewünscht funktioniert hat. Oder ob das überschreiben nicht pseudo-zufällig war? Das Laufwerk mit einem Vorschlaghammer zu zertrümmern ist einfacher, einfach zu kontrollieren, und sehr schwer falsch zu machen.

Das GPL Paket DBAN ist ein Versuch, diese Ungewissheit, ohne Zerstörung der Hardware, zu beseitigen. Hardware-Geräte mit ähnlichen Zielen schliessen den "Drive Erazer" ein; und den "Digital-Shredder".

Alle Hinweise überblickend, stelle ich fest, dass Gutmanns Anspruch in die Kategorie der Urbanen Legenden gehört. Oder er gehört in die Kategorie des Marketing-Hype, denn ich stelle fest, dass er verwendet wird, um ein Softwarepaket zu verkaufen, das "The Annihilator" genannt wird.

Nachdem ich diesen Text geschrieben habe, stiess ich auf einen Kommentar, der Gutmann zugeschrieben wird und der einräumt, dass "moderne" Drives (nach 2003?) nicht mehr mit den im 1996-er Papier beschriebenen Techniken gelesen werden können. Er nimmt aber die übertriebenen Behauptungen des Papiers in Bezug auf ältere Drives nicht zurück. Er nimmt aber die übertriebenen Behauptungen des Papiers in Bezug auf ältere Drives nicht zurück. (http://seclists.org/bugtraq/2005/Jul/0464.html).

Eine modernisierte Kopie dieses Protokolls ist bei http://www.nber.org/sys-admin/overwritten-data-gutmann.html zu finden.

Zusätzliche Information kann an feenberg@nber.org geschickt werden.

Daniel Feenberg
National Bureau of Economic Research

Cambridge MA, USA

21. Juli 2003
24. März 2004 (verbessert)
22. April 2004 (verbessert)
14. Mai 2004 (verbessert)

"Magnetic force microscopy: General principles and application to longitudinal recording media", D.Rugar, H.Mamin, P.Guenther, S.Lambert, J.Stern, I.McFadyen, and T.Yogi, Journal of Applied Physics, Vol.68, No.3 (August 1990), p.1169.

"Magnetic Force Scanning Tunnelling Microscope Imaging of Overwritten Data", Romel Gomez, Amr Adly, Isaak Mayergoyz, Edward Burke, IEEE Trans.on Magnetics, Vol.28, No.5 (September 1992), p.3141.

Wright, C.; Kleiman, D, & Sundhar S. R. S.: (2008) "Overwriting Hard Drive Data: The Great Wiping Controversy". ICISS 2008: 243-257 http://portal.acm.org/citation.cfm?id=1496285 . See also a summary at http://sansforensics.wordpress.com/2009/01/15/overwriting-hard-drive-data/