ESTADO ACTUAL DE LA SEGURIDAD INFORMÁTICA: PROBLEMAS Y DESAFÍOS

3 de setiembre de 2015

Hugo D.Scolnik

hscolnik@fd.com.ar

Se observa el comienzo de una declinación de los ataques clásicos de virus, malware, etc.

Conficker (2008) fue el “último” de los ataques masivos

Y un aumento de código malicioso para MACs, smartphones, dispositivos con Android, …

Ataques a estructuras deficientes de firmas digitales, métodos de autenticación remotos, al protocolo SSL, etc

Hablaremos suscintamente de estos temas

Vulnerabilidades de los sistemas operativos

Top operating systems by vulnerabilities reported in 2014

Operating system	# of vulnerabilities	# of HIGH vulnerabilities	# of MEDIUM vulnerabilities	# of LOW vulnerabilities
Apple Mac OS X	147	64	67	16
Apple iOS	127	32	72	23
Linux Kernel	119	24	74	21
Microsoft Windows Server 2008	38	26	12	0
Microsoft Windows 7	36	25	11	0
Microsoft Windows Server 2012	38	24	14	0
Microsoft Windows 8	36	24	12	0
Microsoft Windows 8.1	36	24	12	0
Microsoft Windows Vista	34	23	11	0
Microsoft Windows RT	30	22	8	0

La situación del mercado financiero, así como la de las empresas e instituciones importantes, es bastante razonable en relación con los ataques convencionales.

Un factor importante son las regulaciones existentes respecto a la seguridad informática. En ese sentido no se observan diferencias fundamentales con lo que sucede en USA, Europa, etc.

Las nuevas amenazas afectan a todos casi por igual.

Muchos ataques se relacionan con la generación deficiente de números aleatorios que se utilizan por ejemplo para:

- obtener claves de RSA para la firma digital
- el método de Diffie-Hellman para intercambio de claves
- curvas elípticas (NSA vs NIST)
- autenticación remota (e-tokens, etc.)
- protocolos de challenge-response
- ataques de canales laterales

Flaw Found in an Online Encryption Method

By JOHN MARKOFF

Published: February 14, 2012

SAN FRANCISCO — A TEAM OF EUROPEAN AND AMERICAN MATHEMATICIANS AND CRYPTOGRAPHERS HAVE DISCOVERED AN UNEXPECTED WEAKNESS IN THE ENCRYPTION SYSTEM WIDELY USED WORLDWIDE FOR ONLINE SHOPPING, BANKING, E-MAIL AND OTHER INTERNET SERVICES INTENDED TO REMAIN PRIVATE AND SECURE.

THE FLAW — WHICH INVOLVES A SMALL BUT MEASURABLE NUMBER OF CASES — HAS TO DO WITH THE WAY THE SYSTEM GENERATES RANDOM NUMBERS, WHICH ARE USED TO MAKE IT PRACTICALLY IMPOSSIBLE FOR AN ATTACKER TO UNSCRAMBLE DIGITAL MESSAGES.

Fuente: http://www.nytimes.com/2012/02/15/technology/researchers-find-flaw-in-an-online-encryption-method.html?pagewanted=all

El paper serio en : http://eprint.iacr.org/2012/064.pdf

Update (2012-02-17): After some investigation and facts that came to light as a result of a parallel experiment by researcher Nadia Heninger at UC San Diego and collaborators at the University of Michigan, it seems the scope of the problem with respect to keys associated with X.509 certificates is limited primarily to certificates that exist for embedded devices such as routers, firewalls, and VPN devices. The small number of vulnerable, valid CA-signed certificates have already been identified and the relevant parties have been notified. Nadia's excellent blog post provides a good overview of the situation right now. We are working with her on disclosure and to provide people with tools to audit against these types of vulnerabilities via the Decentralized SSL Observatory.

Using previously published and new data from EFF's SSL Observatory project, a team of researchers led by Arjen Lenstra at EPFL conducted an audit of the public keys used to protect HTTPS. Lenstra's team has discovered tens of thousands of keys that offer effectively no security due to weak random number generation algorithms.

Fuente: https://www.eff.org/rng-bug

Debian Security Advisory
DSA-1571-1 openssl -- predictable random number generator
13 May 2008

Luciano Bello discovered that the random number generator in Debian's openssl package is predictable. This is caused by an incorrect Debian-specific change to the openssl package (CVE-2008-0166). As a result, cryptographic key material may be guessable.
This is a Debian-specific vulnerability which does not affect other operating systems which are not based on Debian. However, other systems can be indirectly affected if weak keys are imported into them.
It is strongly recommended that all cryptographic key material which has been generated by OpenSSL versions starting with 0.9.8c-1 on Debian systems is recreated from scratch. Furthermore, all DSA keys ever used on affected Debian systems for signing or authentication purposes should be considered compromised; the Digital Signature Algorithm relies on a secret random value used during signature generation.

Fuente: http://www.debian.org/security/2008/dsa-1571

14/05/2008

Graves problemas en el algoritmo que genera los números aleatorios en Debian

---

La criptografía en Debian ha sufrido un grave revés. Se ha descubierto que el generador de números aleatorios del paquete OpenSSL de Debian es predecible. Esto hace que las claves generadas con él ya no sean realmente fiables o verdaderamente seguras. El problema tiene (y tendrá por muchos años) una importante repercusión y numerosos efectos colaterales en otros paquetes y distribuciones.

Debian ha publicado una actualización para OpenSSL que solventa múltiples vulnerabilidades, siendo la más grave un fallo en el generador de números aleatorios que los volvía predecibles, o sea, "poco aleatorios". Luciano Bello, desarrollador de Debian, daba la voz de alarma. Sólo afecta al OpenSSL de Debian porque esta distribución parchea su propia versión de OpenSSL, a su manera. En este caso, ha eliminado una línea crucial de código que limita el generador a producir sólo 2^18 claves (solamente 262.144), en vez de poder elegir claves de, por ejemplo 2^1.024 posibilidades.

How Intel is Solving the Problems with Random Number Generation
Researchers at Intel have devised a new method that produces random numbers in your computer on an unheard of scale. (September 2011)

Random numbers are everywhere in computing. When it comes to simulations, randomness masquerades as what is natural: we can't predict the world, so when we recognize patterns we identify something artificial about our surroundings. Some applications require more randomness than others. Picking the next block that will drop in Tetris or serving up a random Wikipedia page don't require intense number crunching. But encryption algorithms, however, do necessitate random numbers that cannot be predicted. When transmitting secure information, random number generators are used to create the encryption keys used to protect everything from your folder of financial information stored on your local computer to HTTPS data transfers.

Intel "Bull Mountain" hardware random number generator en la arquitectura Ivy Bridge

RISK ASSESSMENT / SECURITY & HACKTIVISM

“We cannot trust” Intel and Via’s chip-based crypto, FreeBSD developers say

Following NSA leaks from Snowden, engineers lose faith in hardware randomness.

Linux supremo Linus Torvalds has snubbed a petition calling for his open-source kernel to spurn the Intel processor instruction RdRand - used for generating random numbers and feared to be nobbled by US spooks to produce cryptographically weak values.

Could RDRAND (Intel) compromise entropy?

In recent years, collision attacks have been announced for many commonly used hash functions, including MD5 and SHA1. This greatly impacts deployments that rely on collision resistance, such as X.509 certificates and SSL. Lenstra and de Weger demonstrated a way to use MD5 hash collisions to construct two X.509 certificates that contain identical signatures and that differ only in the public keys.

NIST recently recommended that Federal agencies stop using SHA-1 for digital signatures, digital time stamping and other applications that require collision resistance.

Por eso SHA-3 . El estándar definitivo está por ejemplo en

http://darkmatters.norsecorp.com/2015/08/11/nist-issues-final-sha-3-cryptographic-hash-standard/

Veamos algo relacionado:

Sea una clave RSA con p = 37, q = 41, n = 1.517, Φ(n) = 1.440, e = 13, d = 997. Vamos a firmar el valor 1.001 con la clave privada e = 13 y luego la verificaremos con la clave pública d = 997.

Cifrado con e = 13: $1.001^{13} \mod 1.517 = 1.088$
Descifrado con d = 997: $1.088^{997} \mod 1.517 = 1.001$.

Se ha verificado la firma digital del mensaje M = 1.001

Pero si usamos los números 277, 637 y 1.357 como si fuesen la clave pública d, obtenemos lo siguiente:
Descifrado con d' = 277: $1.088^{277} \mod 1.517 = 1.001$
Descifrado con d' = 637: $1.088^{637} \mod 1.517 = 1.001$
Descifrado con d' = 1.357: $1.088^{1.357} \mod 1.517 = 1.001$ ...

¡También se ha recuperado el texto en claro o secreto!

Esto tiene que ver con la generación de los números primos p,q

Ataques a Diffie-Hellman (2015)

https://weakdh.org/imperfect-forward-secrecy.pdf

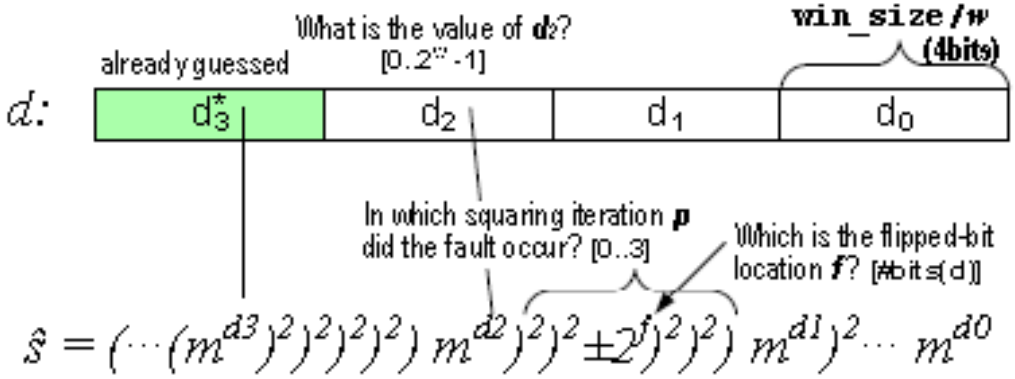
"ABSTRACT: We investigate the security of Diffie-Hellman key exchange as used in popular Internet protocols and find it to be less secure than widely believed. First, we present a novel flaw in TLS (Transport Layer Security) that allows a man-in-the-middle to downgrade connections to “export-grade” Diffie-Hellman. To carry out this attack, we implement the number field sieve discrete log algorithm. After a week-long precomputation for a specified 512-bit group, we can compute arbitrary discrete logs in this group in minutes. We find that 82% of vulnerable servers use a single 512-bit group, allowing us to compromise connections to 7% of Alexa Top Million HTTPS sites. In response, major browsers are being changed to reject short groups. We go on to consider Diffie-Hellman with 768- and 1024-bit groups. A small number of fixed or standardized groups are in use by millions of TLS, SSH, and VPN servers. Performing precomputations on a few of these groups would allow a passive eavesdropper to decrypt a large fraction of Internet traffic. In the 1024-bit case, we estimate that such computations are plausible given nation-state resources, and a close reading of published NSA leaks shows that the agency’s attacks on VPNs are consistent with having achieved such a break. We conclude that moving to stronger key exchange methods should be a priority for the Internet community."

Is NSA Breaking 1024-bit DH?

Our calculations suggest that it is plausibly within NSA's resources to have performed number field sieve precomputations for at least a small number of 1024-bit Diffie-Hellman groups. This would allow them to break any key exchanges made with those groups in close to real time. If true, this would answer one of the major cryptographic questions raised by the Edward Snowden leaks: How is NSA defeating the encryption for widely used VPN protocols?

Ataques por canales laterales:

- Análisis del consumo de energía
- Mantener los datos en RAM mediante congelación
- Análisis acústicos
- Ataques por errores sutiles en los microprocesadores



Example of our private key recovery. The schematic shows a situation where the private key d to be recovered has size 16 bits, and each window is 4 bits long. Key recovery proceeds by determining first the 4 most significant bits in d, d_3.

NSA Preps Quantum-Resistant Algorithms to Head Off Crypto-Apocalypse
Ars Technica (08/21/15) Dan Goodin

The U.S. National Security Agency last week updated the guidance it provides agencies and contractors in regards to the use of cryptography to warn about the possible effects quantum computers could have on modern cryptographic keys and algorithms. **Quantum computers hold the potential to overturn contemporary cryptography by factoring keys almost instantaneously, but most experts believe researchers are a decade, if not decades, away from having a functioning quantum computer**. However, NSA considers the threat imminent enough to start the shift toward what it calls quantum-resistant crypto. In its new guidance, NSA recommends agencies and contractors already using the cryptographic algorithms and key sizes currently recommended by the agency continue to do so, but advises those that have not yet adopted NSA-approved crypto to hold off until the new quantum-resistant crypto standards are ready. "For those partners and vendors that have not yet made the transition to Suite B algorithms, we recommend not making a significant expenditure to do so at this point, but instead to prepare for the upcoming quantum-resistant algorithm transition," NSA says in its guidance. The agency did not say how long it will take for quantum-resistant algorithms to be published, but if it follows the gradual process of previous cryptographic roll-outs, it could be decades before quantum-resistant crypto is widely implemented.

La seguridad o inseguridad del uso de celulares y/o WiFi

El área de Software y Servicios móviles es tal vez la más dinámica e innovadora de las TICs. Los servicios bancarios, financieros y de pagos móviles, los servicios móviles para viajeros y los entornos para la creación y provisión de contenidos basados en los usuarios, son solamente algunos ejemplos bien conocidos de las nuevas direcciones en las aplicaciones de las tecnologías de la información. En efecto, los “usuarios comunes” se vuelven crecientemente creadores y proveedores de contenidos; por cierto, crearlos con las cámaras en sus teléfonos móviles es solamente el comienzo. En este contexto, el tratamiento de la seguridad y la confiabilidad presenta desafíos a nivel de políticas y regulaciones tanto como desafíos tecnológicos.

“Seguridad” en las comunicaciones

El primer punto a considerar es que los celulares son radios, y como tales se pueden escuchar, interferir, etc, y lo análogo sucede con las redes inalámbricas.

Esto dio lugar al desarrollo de métodos de encriptación de las comunicaciones como:

Wired Equivalent Privacy

WEP, acrónimo de ***Wired Equivalent Privacy*** o "Privacidad Equivalente a Cableado", es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite. Proporciona un cifrado a nivel 2, basado en el algoritmo de cifrado RC4 que utiliza claves de 64 bits (40 bits más 24 bits del vector de iniciación IV) o de 128 bits (104 bits más 24 bits del IV). Los mensajes de difusión de las redes inalámbricas se transmiten por ondas de radio, lo que los hace más susceptibles, frente a las redes cableadas, de ser captados con relativa facilidad. Presentado en 1999, el sistema WEP fue pensado para proporcionar una confidencialidad comparable a la de una red tradicional cableada.
Comenzando en 2001, varias debilidades serias fueron identificadas por analistas criptográficos. Como consecuencia, hoy en día una protección WEP puede ser violada con software fácilmente accesible en pocos minutos.

http://www.youtube.com/watch?v=UByyoArzPcQ

WPA-Personal (Wireless Protected Access) :

WPA tiene como objetivo eliminar las vulnerabilidades de

WPA2-Personal: (**la mejor opción**)

WPA y WPA2 se confunden a menudo. La mayor diferencia es que *WAP2 usa AES (Advanced Encryption Standard Algorithm) .*

Comentario muy técnico:

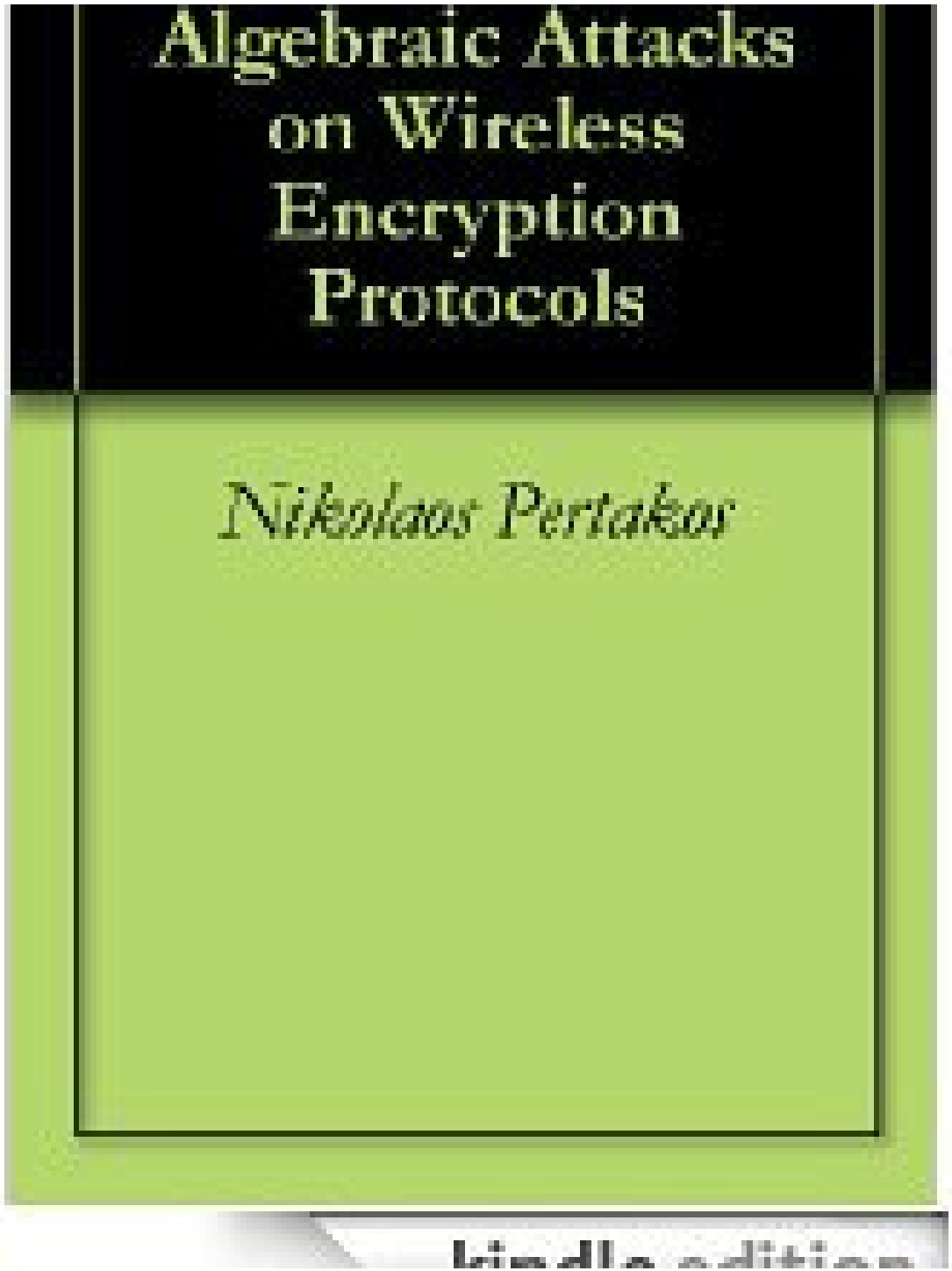
Temporal Key Integrity Protocol or TKIP is a security protocol used in the IEEE 802.11 wireless networking standard. However, researchers have discovered a flaw in TKIP that relied on older weaknesses to retrieve the keystream from short packets to use for re-injection and spoofing.November 6, 2008 See
Battered, but not broken: understanding the WPA crack
WiFi security takes a hit with the disclosure of an effective exploit for small packets encrypted with the TKIP flavor of WiFi Protected Access. The technique is fiendishly clever; the security solution, simple: switch to AES-only in WPA2.
Glenn Fleishman November 6, 2008.

Cube-Type Algebraic Attacks on Wireless Encryption Protocols

October 2009 (vol. 42 no. 10)pp. 103-105
Nikolaos Petrakos, Hellenic Navy
George W. Dinolt, Naval Postgraduate School
James Bret Michael, Naval Postgraduate School
Pantelimon Stanica, Naval Postgraduate School

http://www.computer.org/portal/web/csdl/doi/10.1109/MC.2009.318

En este trabajo se disminuyó la complejidad de atacar protocolos como Bluetooth


Algebraic Attacks on Wireless Encryption Protocols
Nikolaos Pertakos

Borrando datos ……..


NO
MISTAKE
CORRECTION
FLUID

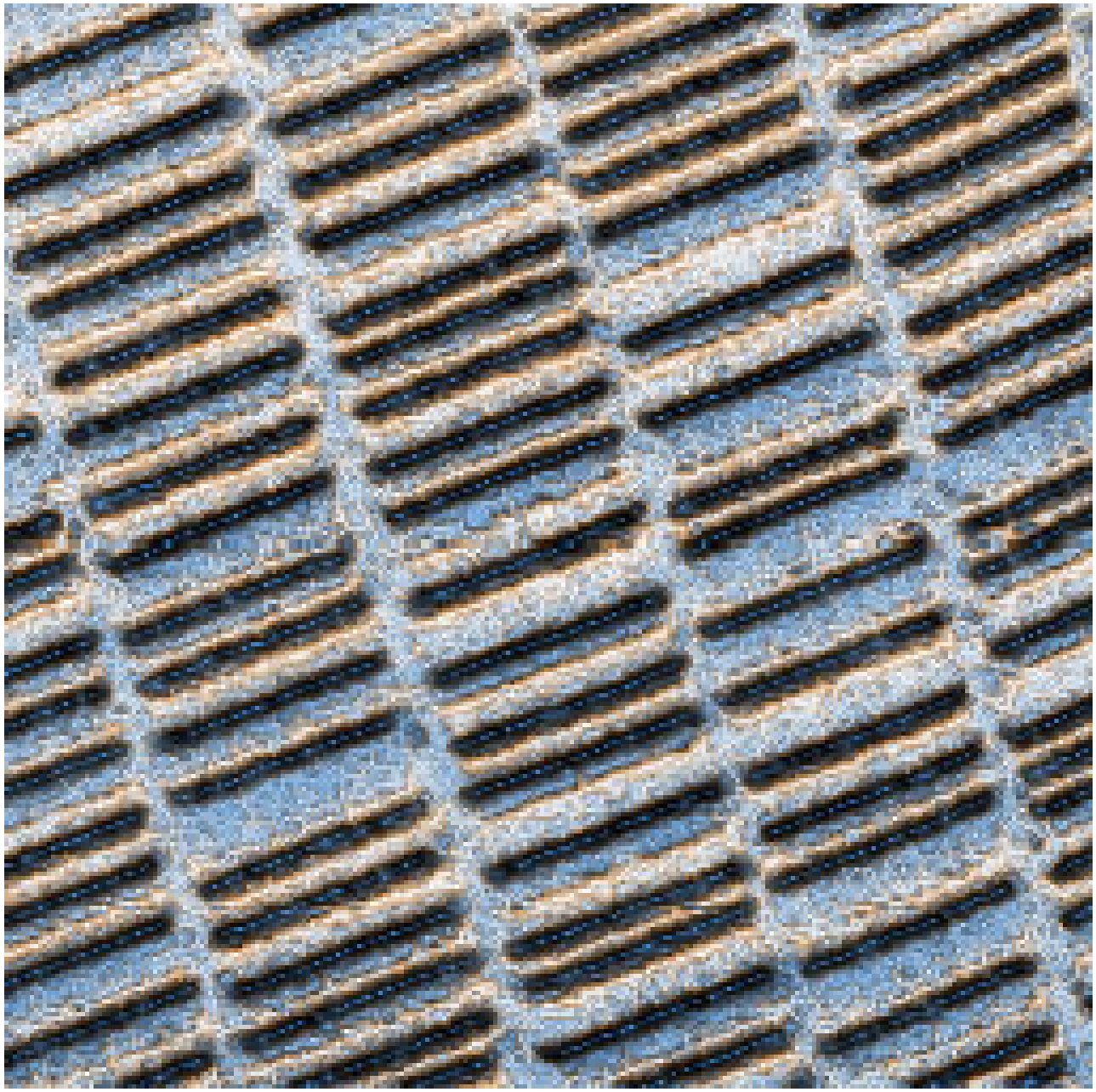
Como es sabido, el simple borrado de un archivo no elimina la información, y existen muchas maneras de recuperarla.

El “borrado seguro” o wiping: sobreescribe el área ocupada por un archivo con ceros, o unos, o caracteres aleatorios, y cada vez más encontramos en las pericias que esta técnica se ha utilizado aún por personal no especializado.

Dado que el simple sobregrabado de ceros no brinda demasiada seguridad en el borrado de información confidencial hay técnicas mucho más sofisticadas como, por ejemplo, el estándar del Departamento de Defensa de EEUU (**DoD 5220.22-M**) que usa tres ciclos de sobregrabación (ceros, unos y bits al azar) y uno final de lectura para verificación. Hay que tener en cuenta que se trata de una operación lenta que puede llevar horas con un disco rígido de la capacidad actual, por eso no puede ser empleada bajo condiciones de apremio temporal. Hay otros estándares aún más exigentes como el **GUTMANN** que hace 35 ciclos de sobregrabación de ceros y unos aleatorios (http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html).

Pero, qué sucede al grabar y sobregrabar ? Cuando los datos se escriben las cabezas del disco definen la polaridad de la mayoría de los dominios magnéticos, pero no de todos. El efecto de sobreescribir un 0 con un 1 da aproximadamente 0.95, y el de sobreescribir un 1 con otro 1 da aproximadamente 1.05. Los equipos de lectura normales interpretan ambos como un 1, pero con equipos muy especializados es posible descubrir la historia de la sobregrabación.

Asimismo existen las técnicas de nanotecnología modernas como Scanning Probe Microscopy (SPM) y su seguidor Magnetic Force Microscopy (MFM) que permiten conseguir imágenes como



derivadas de la magnetización remanente de los bordes de las pistas de los discos, y que forman una “fotografía” de la historia de grabación.

También se usan aparatos llamados “degaussers” para borrar información como

Por eso dice J.J.Sawyer, un conocido experto de Estados Unidos:

Hasta hace poco tiempo se creía que wipear reiteradamente una misma área del disco eliminaba todas las posibilidades de recuperación, y por eso el Departamento de Defensa de los Estados Unidos había generado el estándar DoD (directiva DoD 5220.22-M-Sup 1 Chapter 8, “Degaussing is more reliable than overwriting magnetic media.” (DoD, 2005, pág.18).) recomendando repetir el proceso siete veces (y otros científicos llegaron a promover treinta y tres “pasadas”).

Hoy en día para proteger los archivos “Top Secret” la **única** recomendación **es destruir el disco.**

En el mundo existen diversos laboratorios para efectuar los análisis forenses de medios magnéticos, en general pertenecientes a gobiernos, pero hay algunos privados.

E-MAIL

hscolnik@fd.com.ar