¿Quién necesita ordenadores cuánticos?

Fernando Martínez

Departament de Matemàtiques • Universitat Politècnica de Catalunya

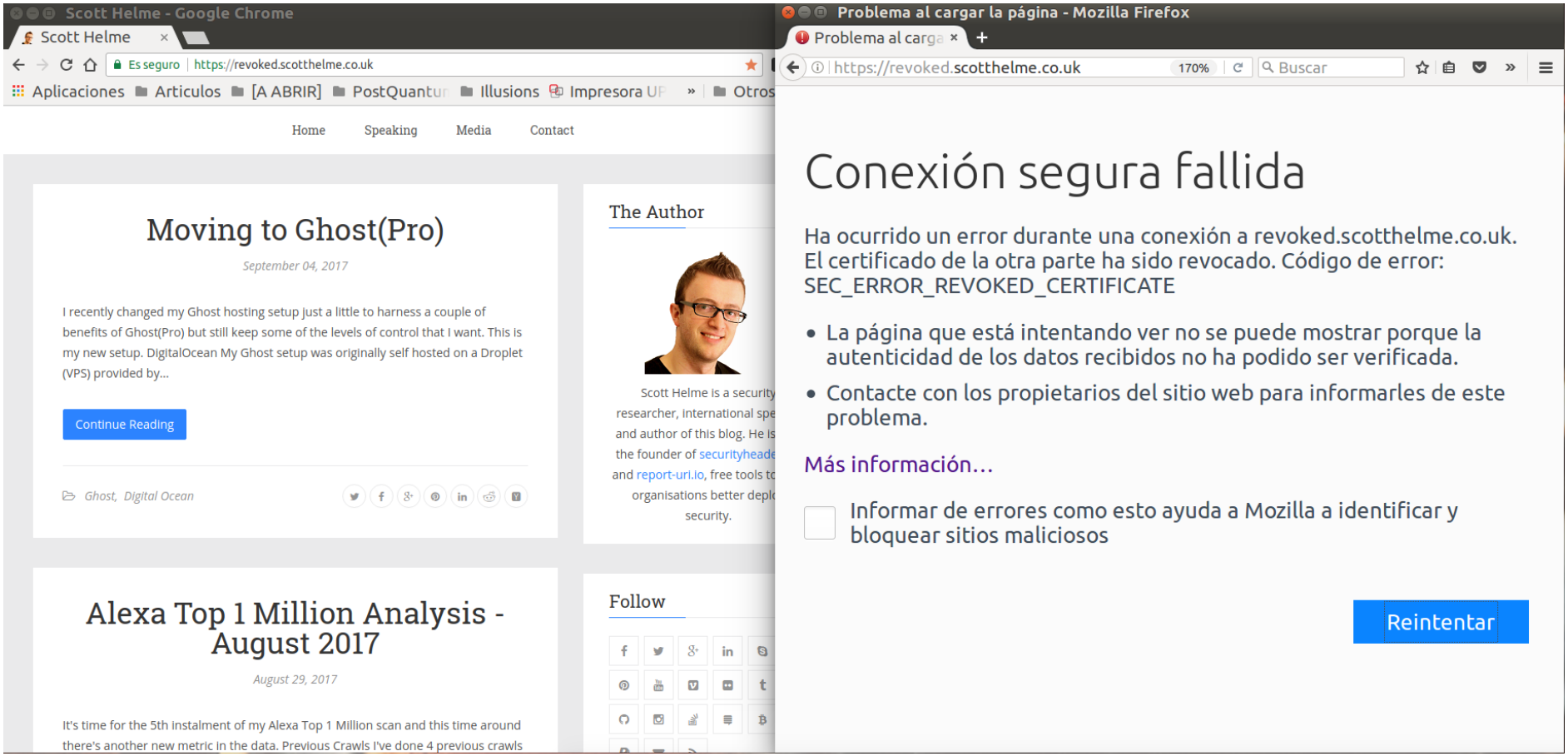
7 de octubre de 2017

Índice

Certificado digital

Certificado digital: documento electrónico que asocia una clave pública con su propietario.

- Redes de confianza: PGP.
- Autoridades certficadoras: X509.


Scott Helme - Google Chrome
Scott Helme
Es seguro | https://revoked.scotthelme.co.uk
Aplicaciones Articulos [A ABRIR] PostQuantur Illusions Impresora UP Otros
Home Speaking Media Contact
Moving to Ghost(Pro)
September 04, 2017
I recently changed my Ghost hosting setup just a little to harness a couple of benefits of Ghost(Pro) but still keep some of the levels of control that I want. This is my new setup. DigitalOcean My Ghost setup was originally self hosted on a Droplet (VPS) provided by...
Continue Reading
Ghost, Digital Ocean
The Author
Scott Helme is a security researcher, international spe and author of this blog. He is the founder of securityheade and report-uri.io, free tools to organisations better deplo security.
Alexa Top 1 Million Analysis - August 2017
August 29, 2017
It's time for the 5th instalment of my Alexa Top 1 Million scan and this time around there's another new metric in the data. Previous Crawls I've done 4 previous crawls
Follow
Problema al cargar la página - Mozilla Firefox
Problema al carga
https://revoked.scotthelme.co.uk 170% Buscar
Conexión segura fallida
Ha ocurrido un error durante una conexión a revoked.scotthelme.co.uk. El certificado de la otra parte ha sido revocado. Código de error: SEC_ERROR_REVOKED_CERTIFICATE
La página que está intentando ver no se puede mostrar porque la autenticidad de los datos recibidos no ha podido ser verificada.
Contacte con los propietarios del sitio web para informarles de este problema.
Más información…
Informar de errores como esto ayuda a Mozilla a identificar y bloquear sitios maliciosos
Reintentar

- *Microsoft Security Bulletin MS01-017 (22/3/2001):* In mid-March 2001, VeriSign, Inc., advised Microsoft that on January 29 and 30, 2001, it issued two VeriSign Class 3 code-signing digital certificates to an individual who fraudulently claimed to be a Microsoft employee.

- *Comodo SSL Affiliate The Recent RA Compromise (23/3/2011)*
  On March 15th 2011, a Comodo affiliate RA was compromised resulting in the fraudulent issue of 9 SSL certificates to sites in 7 domains. Although the compromise was detected within hours and the certificates revoked immediately, the attack and the suspected motivation require urgent attention of the entire security field. 9 certificates were issued:
  - NOT seen live on the internet: mail.google.com, www.google.com, login.yahoo.com (2), login.skype.com, addons.mozilla.org, login.live.com, global trustee.
  - Seen live on the internet: login.yahoo.com,

  The incident report

- *DigiNotar reports security incident (30/8/2011)* On July 19th 2011, DigiNotar detected an intrusion into its Certificate Authority (CA) infrastructure, which resulted in the fraudulent issuance of public key certificate requests for a number of domains, including Google.com.

  An update on attempted man-in-the-middle attacks

- *EFF to Verizon: Etisalat Certificate Authority Threatens Web Security (13/8/2010)* We are writing to request that Verizon investigate the security and privacy implications of the SSL CA certificate (serial number 0x40003f1) that Cybertrust (now a division of Verizon) issued to Etisalat on the 19th of December, 2005, and evaluate whether this certificate should be revoked.[...] These events clearly demonstrate that Etisalat and the UAE regulatory environment within which it operates are institutionally hostile to the existence and use of secure cryptosystems. It is therefore of great concern to us that Etisalat is in possession of a trusted SSL CA certificate and the accompanying private key, which effectively functions as a master key for the encrypted portion of the World Wide Web. Etisalat could use this key to issue itself valid HTTPS certificates for verizon.com, eff.org, google.com, microsoft.com, or indeed any other website. Etisalat could use those certificates to conduct virtually undetectable surveillance and attacks against those sites. Etisalat's keys could also possibly be used to obtain access to some corporate VPNs.

- *Win32/Stuxnet Signed Binaries (19/7/2010)* On July 17th, ESET identified a new malicious file related to the Win32/Stuxnet worm. This new driver is a significant discovery because the file was signed with a certificate from a company called `JMicron Technology Corp`. This is different from the previous drivers which were signed with the certificate from `Realtek Semiconductor Corp`. It is interesting to note that both companies whose code signing certificates were used have offices in Hsinchu Science Park, Taiwan.

- *Adobe Reader zero-day attack - now with stolen certificate (8/9/2010)* While most malicious PDFs download their payload, this time the PDF has malicious content embedded. The PDF drops an executable into the `temp` directory and tries to execute it. The file it drops is digitally signed with a valid signature from a `US-based Credit Union`!

- *How a 2011 Hack You've Never Heard of Changed the Internet's Infrastructure.* It all started with an internet user in Iran who couldn't get into his Gmail account.

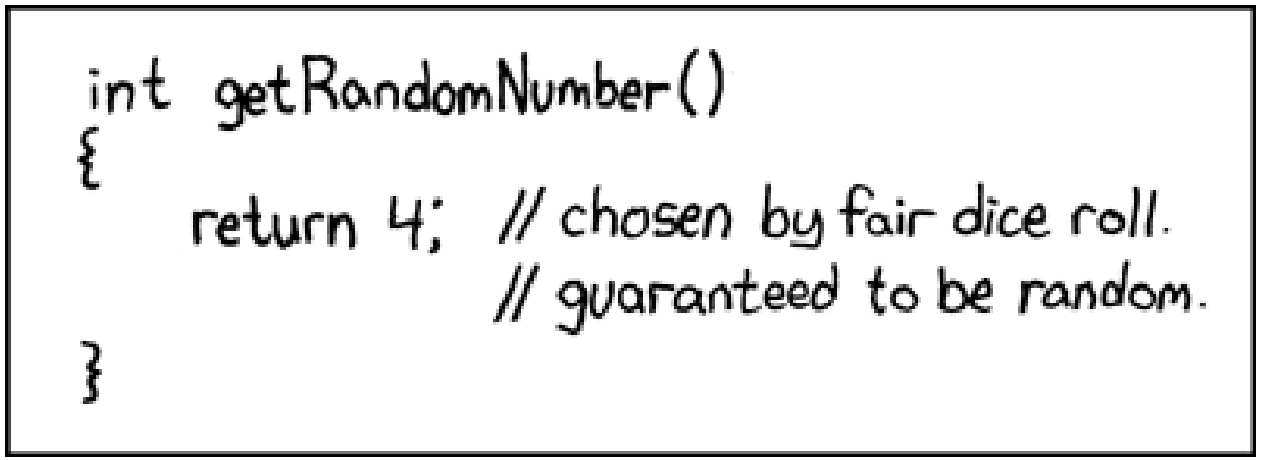
- *Ron was wrong, Whit is right. (14 Feb 2012)* We performed a sanity check of public keys collected on the web. Our main goal was to test the validity of the assumption that different random choices are made each time keys are generated. We found that the vast majority of public keys work as intended. A more disconcerting finding is that **two out of every one thousand RSA moduli that we collected offer no security.** Our conclusion is that the validity of the assumption is questionable and that generating keys in the real world for ”multiple-secrets” cryptosystems such as RSA is significantly riskier than for ”single-secret” ones such as ElGamal or (EC)DSA which are based on Diffie-Hellman.

Factoring one 1024-bit RSA modulus would be historic. Factoring 12720 such moduli is a statistic.

- *Widespread Weak Keys in Network Devices (2012)*
  - We found that 5.57 % of TLS hosts and 9.60 % of SSH hosts share public keys in an apparently vulnerable manner, due to either insufficient randomness during key generation or device default keys.
  - We were able to remotely obtain the RSA private keys for 0.50 % of TLS hosts and 0.03 % of SSH hosts because their public keys shared nontrivial common factors due to poor randomness.
  - We were able to remotely obtain the DSA private keys for 1.03 % of SSH hosts due to repeated signature randomness.[1]

[1] PS3 Security Broken. PS3 Epic Fail (2010)
https://events.ccc.de/congress/2010/Fahrplan/events/4087.en.html
https://events.ccc.de/congress/2010/Fahrplan/attachments/1780_27c3_console_hacking_2010.pdf

xkcd Random Number



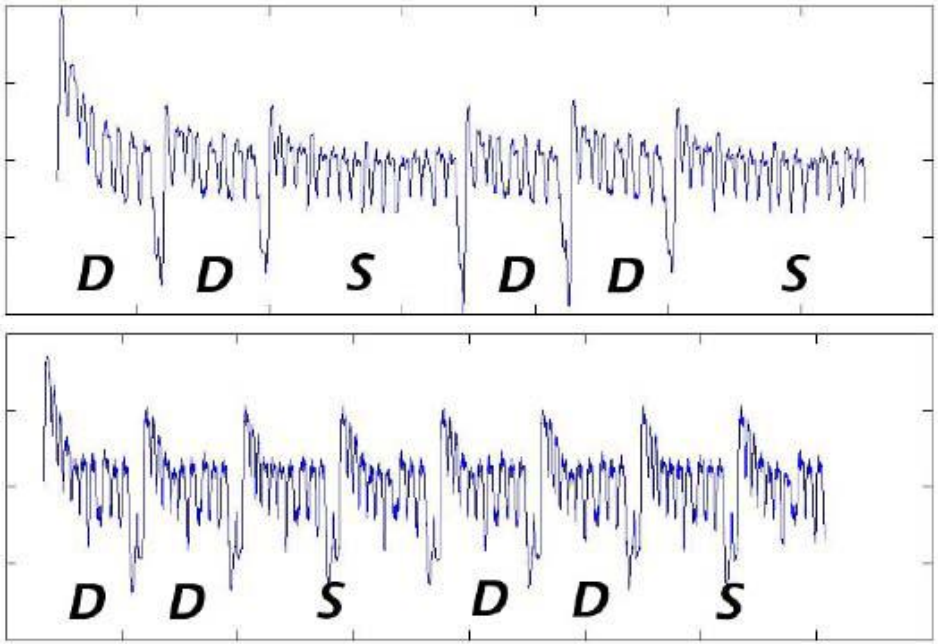
- DSA-1571-1 openssl – predictable random number generator (13 May 2008) Luciano Bello discovered that the random number generator in Debian's openssl package is predictable. This is caused by an incorrect Debian-specific change to the openssl package (CVE-2008-0166). As a result, cryptographic key material may be guessable.
- *When Private Keys are Public: Results from the 2008 Debian OpenSSL Vulnerability (November 2009)* Beginning in September, 2006 the package for OpenSSL included in the Debian distribution of Linux was modified to incorporate a bugfix intended to eliminate uninitialized memory reads flagged by the memory checking tool Valgrind. The bugfix did not just this but more: it eviscerated OpenSSL's entropy gathering. Until the problem was noticed by Luciano Bello in May of 2008, the entropy available to applications running on Debian (and Debian-derived distributions, such as Ubuntu) was severely constrained.

- *The Debian OpenSSL Bug: Backdoor or Security Accident? (September 20, 2013)* At the very least, transparency lets us look back, years later, and figure out what caused the bug– in this case, engineering error and not deliberate sabotage.
- ITL (NIST) is taking the following actions: Recommending against the use of SP 800-90A Dual Elliptic Curve Deterministic Random Bit Generation (09/09/2013)
- Stop using NSA-influenced code in our products, RSA tells customers (20/09/2013)
- The NSA apparently paid RSA $10M to use Dual EC random number generator. (21/12/2013)

- *The Debian OpenSSL Bug: Backdoor or Security Accident? (September 20, 2013)* At the very least, transparency lets us look back, years later, and figure out what caused the bug– in this case, engineering error and not deliberate sabotage.
- ITL (NIST) is taking the following actions: Recommending against the use of SP 800-90A Dual Elliptic Curve Deterministic Random Bit Generation (09/09/2013)
- Stop using NSA-influenced code in our products, RSA tells customers (20/09/2013)
- The NSA apparently paid RSA $10M to use Dual EC random number generator. (21/12/2013)

- Impementación SAGE[2] de On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng, Dan Shumow and Niels Ferguson (2007) https://rump2007.cr.yp.to/15-shumow.pdf

[2] PowmInsecureWarning: Not using mpz_powm_sec. You should rebuild using libgmp >= 5 to avoid timing attack vulnerability.



- Bleichenbacher's RSA signature forgery based on implementation error, 2006 https://www.ietf.org/mail-archive/web/openpgp/current/msg00999.html
- Bleichenbacher's CCA attack on PKCS#1 v1.5 http://archiv.infsec.ethz.ch/education/fs08/secsem/bleichenbacher98.pdf
- D. Boneh, R.A. DeMillo, and R.J. Lipton. *On the Importance of Checking Cryptographic Protocols for Faults*, EUROCRYPT 1997 https://pdfs.semanticscholar.org/7622/200b9459a8c0e25e74ce7316c2402862e919.pdf
- Factoring as a Service http://eprint.iacr.org/2015/1000

- Elige e igual a 65537 $(2^{16}+1)$ cifrar e igual a 3 (2^1+1) para firmar.
- p y q primos aleatorios diferentes con $(e, p-1) = 1$, $(e, q-1) = 1$.
- $n = pq$.
- $d = e^{-1} \mod MCM(p-1, q-1)$.

$$\begin{array}{ll} d_p \equiv d \mod (p-1), & p_{inv} \equiv p^{-1} \mod q, \\ d_q \equiv d \mod (q-1), & q_{inv} \equiv q^{-1} \mod p, \end{array}$$

- Descifrado
  $m_p = c^{d_p} \pmod p$ y $m_q = c^{d_q} \pmod q$, resuelve el sistema:

$$\left.\begin{array}{ll} m \equiv m_p & \mod p \\ m \equiv m_q & \mod q \end{array}\right\} m = m_p q_{inv} q + m_q p_{inv} p \mod n.$$

  Resolver el sistema es equivalente a $h \equiv (m_p - m_q) q_{inv} \mod p$ y

$$m = m_q + q\, h \mod n$$

- Clave pública $\{e, n\}$. Clave privada $\{d, p, q, d_p, d_q, q_{inv}\}$.

SLE 66CX322P 136-Kbytes ROM, 5052 bytes RAM, 32-Kbytes EEPROM

Operation	**Modulus**	**Exponent**	**Calculation Time**		
			5 MHz	10 MHz	15 MHz
RSA Encrypt / Signature Verify	1024 bit 2048 bit	17 bit 17 bit	20 ms 630 ms	11 ms 315 ms	7 ms 210 ms
RSA Decrypt / Signature Generate	1024 bit	1024 bit	820 ms	410 ms	273 ms
RSA Decrypt / Signature Generate using CRT	eq.1024 bit eq.2048 bit	eq.1024 bit eq.2048 bit	250 ms 1840 ms	125 ms 920 ms	83 ms 614 ms
DSA Signature Generate	512 bit	160 bit	97 ms	49 ms	32 ms
DSA Signature Verify	512 bit	160 bit	117 ms	59 ms	39 ms
DSA Signature Generate	1024 bit	160 bit	438 ms	219 ms	146 ms
DSA Signature Verify	1024 bit	160 bit	711 ms	356 ms	237 ms

Operation	**Data Block Length**	**Encryption time, incl. data transfer**		
		5 MHz	10 MHz	15 MHz
56-bit Single DES Encryption	64 bit	23 μs	11 μs	8 μs
112-bit Triple DES Encryption	64 bit	35 μs	17 μs	12 μs

Operation	**Operand Length**	**Calculation Time**		
		5 MHz	10 MHz	15 MHz
EC-DSA GF(2^n) Signature Generate	192 bit	285 ms	142 ms	95 ms
EC-DSA GF(2^n) Signature Verify	192 bit	540 ms	270 ms	180 ms

Cracking Passwords

- John the Ripper
- ophcrack
- RainbowCrack
- Frequent password changes are the enemy of security, FTC technologist says