# SEMINARIO REGIONAL DE CIBERDEFENSA

**14 al 16-Mayo-2014**

# La criptografía como escudo para la ciberdefensa

**Dr. Hugo Daniel Scolnik**

hscolnik@gmail.com

hugo@dc.uba.ar

# LAS AMENAZAS…

# ¿¿¿SON REALES???


NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA


UNITED STATES CYBER COMMAND

The Washington Post



# $52.6 billion

# The Black Budget

Covert action. Surveillance. Counterintelligence. The U.S. "black budget" spans over a dozen agencies that make up the National Intelligence Program.

The Washington Post SHARE

## 107,035 employees in the intelligence community

**CIA employs the most civilian FTEs: 21,459**

equals 100

83,675
**Full-time equivalent (FTE) civilian employees**

**NSA employs 64 percent of all military personnel in the program: 14,950**

23,400
**Military positions**

21,800
**Full-time contractors**

The number refers to contractors who occupy fu
category generally does not include employees

Scolnik-Ciberdefensa (2014)





CNNMoney FORTUNE

Home | Video | Markets | Investing | E

Apple 2.0 | Big Tech | Tech Tumblr | Innovation Nation | Startups | Brainstorm Tech

IT'S NEVER BEEN DO

# NSA wants to hire hackers

CNNMoney

By Stacy Cowley @CNNMoneyTech July 29, 2012: 10:29 AM ET

LAS VEGAS (CNNMoney) -- Wearing a t-shirt and jeans, America's top spymaster -- National Security Agency Director Gen. Keith Alexander, also the head of the U.S. Cyber Command -- took the stage Friday at the nation's largest hacker convention to deliver a recruiting pitch.

"In this room, this room right here, is the talent our nation needs to secure cyberspace," Alexander told the standing-room-only audience at DefCon, a grassroots gathering in Las Vegas expected to draw a record 16,000 attendees this year. "We need great talent. We don't pay as high as everybody else, but we're fun to be around."

Alexander's appearance is a milestone for DefCon, a hacker mecca with an often-uneasy relationship with the feds. DefCon is the older, wilder and far less official

Sign In SUBSCRIBE: Home Delivery | Digital

The Washington Post | PostTV | Politics | Opinions | Local | Sports

wp POLITICS

# NSA is looking for a few good hackers

By Tabassum Zakaria, August 02, 2011

The National Security Agency has a challenge for hackers who think they by working on the "hardest problems on Earth."

Computer hacker skills are in great demand in the U.S. government to fight the cyberwars that pose a growing national security threat — and they are in short supply.

For that reason an alphabet soup of federal agencies — DOD, DHS, NASA, NSA — are descending on Las Vegas this week for Defcon, an annual hacker convention where the $150 entrance fee is cash only — no registration, no credit cards, no names taken. Attendance is expected to top 10,000.

theguardian

News | Sport | Comment | Culture | Business | Money | Life & style

News › World news › The NSA files

# NSA monitored calls of 35 world leaders after US official handed over contacts

- Agency given more than 200 numbers by government official
- NSA encourages departments to share their 'Rolodexes'
- Surveillance produced 'little intelligence', memo acknowledges

Follow The NSA Files by email BETA

**James Ball**
The Guardian, Friday 25 October 2013

IEEE SPECTRUM

Follow on:

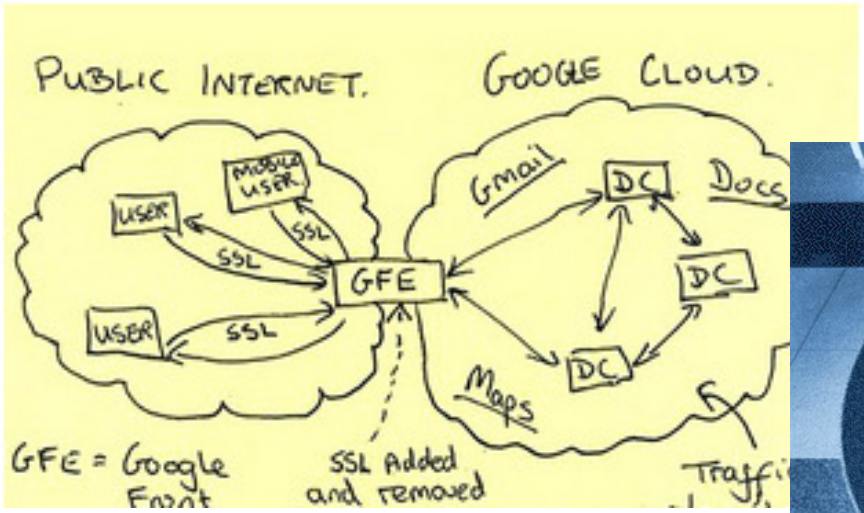
Engineering Topics  Specia

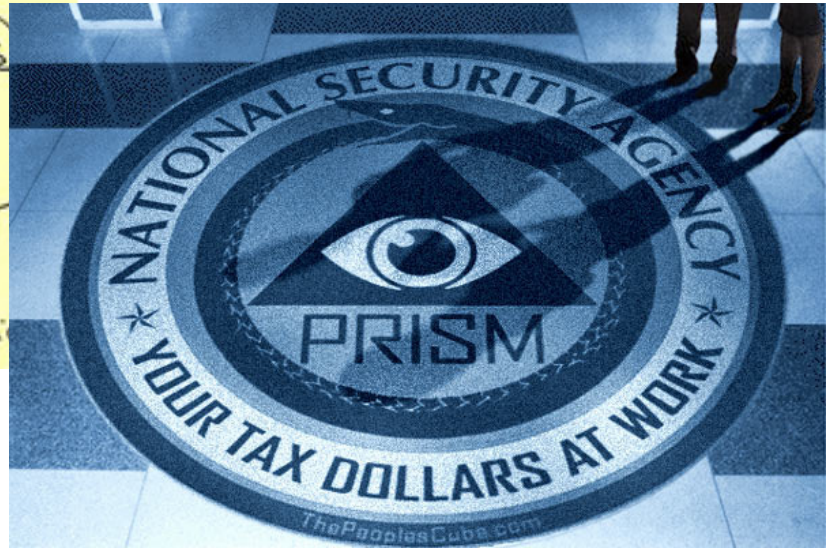
Tech Talk | Telecom | Internet

# NSA Intercepts Links to Google, Yahoo Data Centers

By Jeremy Hsu
Posted 1 Nov 2013 | 14:20 GMT

Share | Email | Print




Scolnik-Ciberdefensa (2014)

Arabic Spanish Russian Freevideo ИНОТВ RTД RUPTLY

RT QUESTION MORE. LIVE

News USA Russian politics Business Op-Edge In vision In moti

Home / USA /

# Snowden leaks: NSA conducted 231 offensive cyber-ops in 2011, hailed as 'active defense'

Published time: August 31, 2013 11:11 Get short URL

# ATAQUES CRIPTOLÓGICOS ENCUBIERTOS…

# Puertas traseras:

## (hay amplios antecedentes documentados en la web)

- Hardware
- Software

NETWORKWORLD News | Blogs | Newsletters | Videos | Events | Resources | INSIDE

Security | LANs & WANs | UC / VoIP | Cloud | Infrastructure Mgmt | Wireless | Software | Data Center

Anti-malware | Compliance | Cybercrime | Firewall & UTM | IDS/IPS | Endpoint Security | SIEM | White Pape

News

# NSA backdoor fears creating crisis of confidence i U.S. high-tech products, services

Intel's CISO: We don't support any backdoors

By Ellen Messmer, Network World
October 09, 2013 01:39 PM ET

10 Comments Print

# *New York Times* provides NSA backdoor in crypto sp

The paper points a finger definitively at the long-suspec

Network World - Fear convince U.S.-based for espionage purpos

There has been, of c documents leaked by neither the NSA nor t has frequently been t

by **Megan Geuss** - Sept 11 2013, 12:00am -0300

Today, the *New York Times* reported that an algorithm for generating random numbers, which was adopted in 2006 by the National Institute of Standards and

# Cisco says controversial NIST crypto - potential NSA backdoor -- 'not invoked' in products

But Cisco engineer says "some of the libraries" in products can support Dual EC DRBG

By Ellen Messmer, Network World
October 17, 2013 03:48 PM ET

1 Comment Print Share 5 Like 0

Network World - Controversial crypto technology known as Dual EC DRBG, thoug be a backdoor for the National Security Agency, ended up in some Cisco products part of its code libraries. But Cisco says they cannot be used because it chose an crypto as an operational default which can't be changed.

Dual EC DRBG or Dual Elliptic Curve Deterministic Random Bit Generator (Dual E DRBG) from the National Institute of Standards and Technology and a crypto toolk RSA is thought to have been one main way the crypto ended up in hundreds of ver

Slashdot Search this website ...

Business Intelligence Cloud DataCenter

# RSA Security Warns of Possible NSA Backdoor

LONGFORM . VIDEO . REVIEWS . TECH . SCIENCE . CULTURE . DESIGN . BUSINESS . US & WOR

# RSA tells developers to stop using encryption with suspected NSA backdoor

By Jeff Blagdon on September 20, 2013 04:33 pm Email @blagdon

DON'T MISS STORIES FOLLOW THE VERGE Like 192k Follow 305K followers


Snowden's NSA post in Hawaii failed to install "anti-leak" software

# *New York Times* provides new details about NSA backdoor in crypto spec

The paper points a finger definitively at the long-suspected Dual_EC_DRBG algorithm.

by **Megan Geuss** - Sept 11 2013, 12:00am -0300

HACKING PRIVACY 85

Today, the *New York Times* reported that an algorithm for generating random numbers, which was adopted in 2006 by the National Institute of Standards and Technology (NIST), contains a backdoor for the NSA. The news followed a *NYT* report from last week, which indicated that the National Security Agency (NSA) had

NSA LEAKS

Snowden's NSA post in Hawaii failed to install "anti-leak" software

# Fallas (y ataques):

- **Hardware**
  - » caso INTEL (testing)
  - » casuales (o no tanto…) errores en CPU
- **Software**
  - » caso NETSCAPE
  - » caso Debian/OpenSSL (Luciano Bello EST)
  - » caso Dual Elliptic Curve RG (RSA Bsafe)
  - » Heartbleed (openSSL)

¿ y el próximo en descubrirse cuál será ?

# Importancia de los generadores seudoaleatorios…


Ej: p.q=n (módulo RSA)

# Récord de quiebre de RSA768 obtenido el 12 de diciembre de 2009

**123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214341 3.**

**Los factores son:**

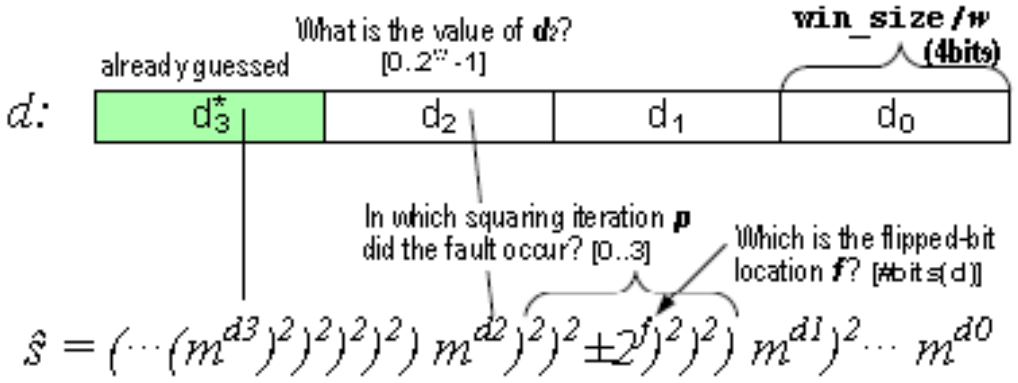
**334780716989568987860441698482126908177047949837137685689124313889828837938780022876147116525317430877378144679994893674604366679959042824463379962795263227915816434308764267603228381573966651127923337341714339681027009279873630891 7**

https://documents.epfl.ch/users/l/le/lenstra/public/papers/rsa768.txt

# Desafío no resuelto: RSA 1024

135066410865995223349603216278805969938881475605667027524485143851526510604859533833940287150571909441798207282164471551373680419703964191743046496589274256239341020864383202110372958725762358509643110564073501508187510676594629205563685529475213500852879416377328533906109750544334999811150056977236890927563

# Importancia de las fallas de CPU (casuales y de las otras…)




**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 $d$, $d_3$.

…recuperando claves privadas a partir de firmas digitales calculadas con defectos de pocos bits

# Importancia de las fallas no detectadas en código abierto (software gratuito… o no tanto!)


Scolnik-Ciberdefensa (2014)

# Conclusiones:

- Sistemas- 100% auditables (hard o soft)
- Control de calidad total (cero falla)
- Desarrollos regionales para cubrir intereses compartidos
- Es vital asegurar las comunicaciones (mail, radios, etc.)