**ISO/IEC JTC 1**
**Information technology**
**Secretariat: ANSI (United States)**

**Document type:** Officer's Contribution

**Title:** REVISED SC 27 Chairman's Presentation to the November 2013 JTC 1 Plenary

**Status:** This document is circulated for review and consideration at the November 2013 JTC 1 Plenary meeting in France.

**Date of document:** 2013-10-18

**Source:** SC 27 Chairman

**Expected action:** ACT

**Action due date:** 2013-11-04

**Email of secretary:** lrajchel@ansi.org

**Committee URL:** http://isotc.iso.org/livelink/livelink/open/jtc1

# SC 27 Update –
## *Intentional Weaknesses in Crypto Standards?*

Walter Fumy, SC 27 Chairman

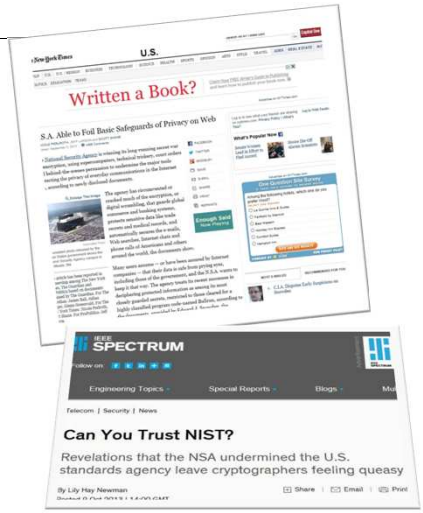
Walter.Fumy@bdr.de

JTC 1 Plenary Meeting
Perros-Guirec, November 2013

## Discussion in the Media

In recent weeks there has been much discussion in both the press and in academic circles regarding intentional weaknesses in crypto standards.

- *"The agency has influenced the international standards upon which encryption systems rely"*
- *"NSA has been introducing weaknesses into security standards, a fact confirmed for the first time by another secret document* [provided by Edward Snowdon]. *It shows the agency worked covertly to get its own version of a draft security standard issued by the US National Institute of Standards and Technology approved for worldwide use in 2006. 'Eventually, NSA became the sole editor,' the document states."*



## Agenda

- Some Crypto Basics
  - Computing Power
  - Key Length Recommendations
- Possibly Flawed Mechanisms
- Recommendations / Way Forward
- Conclusion



## Petascale Computing Available
*Exascale Computing on the Horizon*

Today's most powerful known computer systems include

- Tianhe-2: > 30 petaflops [$10^{16}$ floating point operations per second]

Personal computing

- Intel i7 980 XE: 109 gigaflops [~$10^{11}$ flops]
- ATI Radeon R800 GPU: 3 teraflops [$3 \cdot 10^{12}$ flops]

Distributed computing projects

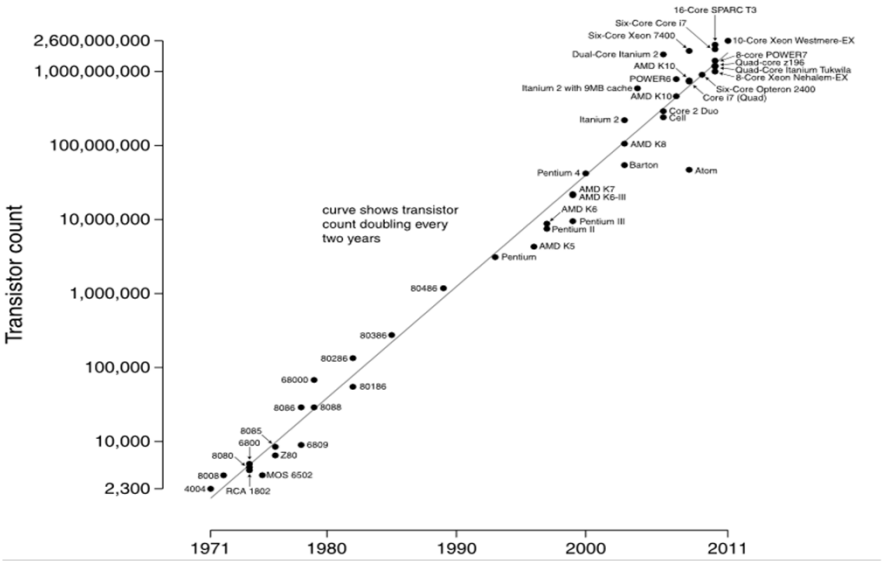
- Folding@Home averages > 6 petaflops from around 400.000 active machines (CPUs, GPUs, Playstations)
- BOINC network: 9.5 petaflops

Given the current speed of progress, supercomputers capable of performing

- exaflops [$10^{18}$ flops] are expected for 2019
- zettaflops [$10^{21}$ flops] are expected for 2030 –

*"zettaflop computing would allow full weather modeling to cover a two week time span accurately"*

## CPU Transistor Count & Moore's Law




Source: Wikipedia

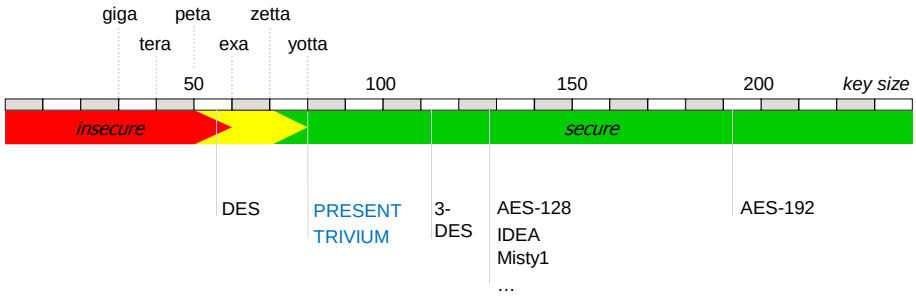
## Orders of Magnitude


6

## Orders of Magnitude (II)


7

## Symmetric Key Lengths



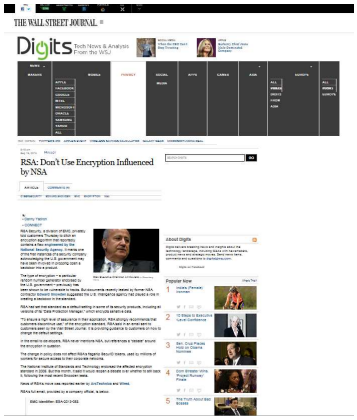

- size matters !!!
- time* matters too
  - A machine that cracks a 56-bit DES key in 1 second would take 149 trillion years to crack a 128-bit key …
  - Main threat are implementation level attacks (aka side channel attacks)

*Note: a standard year has 31.556.926 seconds*

## Dealing with Encryption

To deal with encryption, agencies may

- work with security product vendors to subvert the underlying cryptography, e.g.
  - make the random number generator less random, thus reducing effective key lengths
  - implant backdoors which leak the key somehow
- work with standards bodies to promote weak algorithms
- leverage secret mathematical breakthroughs
- construct quantum computers
- …




9

## Dual_EC_DRBG
## *Flawed Deterministic Random Bit Generation*

- NIST Special Publication 800-90:2006 includes four different algorithms called "deterministic random bit generators," or DRBGs.
- Documents provided by Edward Snowden indicate the NSA played a crucial role in writing NIST SP 800-90.
- Possible weaknesses were identified in one of the algorithms specified, the Dual Elliptic Curve Deterministic Random Bit Generation (Dual_EC_DRBG) scheme.
- NIST recently has recommended that Dual_EC_DRBG should not be used, see http://csrc.nist.gov/publications/nistbul/itlbul2013_09_supplemental.pdf
  *"Concern has been expressed about one of the DRBG algorithms in SP 800-90/90A and ANS X9.82: the Dual Elliptic Curve Deterministic Random Bit Generation (Dual_EC_DRBG) algorithm. This algorithm includes default elliptic curve points for three elliptic curves […], recent community commentary has called into question the trustworthiness of these default elliptic curve points."*
- Dual_EC_DRBG is also specified in ANS X9.82 and in the current (2011) edition of ISO/IEC 18031: Random bit generation.
- Dual_EC_DRBG is included in many cryptographic libraries (e.g., offered by Microsoft, Cisco, Symantec and RSA).

## Recommendations / Way Forward

Dual_EC_DRBG

- Formulate and circulate a draft corrigendum to ISO/IEC 18031:2011 with the effect of removing the Dual_EC_DRBG scheme from the standard.
- Issue a statement advising all users of the scheme to replace it.

General

- Analyze the portfolio of crypto mechanisms for mechanisms that may have been influenced to introduce weaknesses.
- Ensure a sufficient amount of independent cryptographic research.
- Fight a general mistrust in NIST proposals – do not forget NIST has done a great job with cryptographic competitions, both a decade ago with the AES and recently with SHA-3.
- ISO can (and should) play a vital role in the restoration of trust in cryptography and cryptographic security, because ISO provides an open, free and independent framework for assessing security of cryptographic mechanisms.



## Conclusion

Cryptography ≠ security

- crypto is only a tiny (yet very important) piece of the security puzzle
- most systems break elsewhere
- encryption works – if properly implemented
  - closed-source software is easier to backdoor than open-source software
  - proprietary mechanisms are easier to backdoor than ISO standards

Challenges for smart cryptography

- trustworthy software and hardware implementations
- upgrading implemented algorithms
- linking crypto with the physical world
  ⇨ biometrics
  ⇨ physical uncloneable functions
- ISO standards development by cooperating more closely with academic circles and related organizations

## Final Words

"*Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin.*"
-- John von Neumann, 1951

"*You can't trust code that you did not totally create yourself.*"
-- Ken Thompson, Turing Award Lecture 1983

"*Dowjerjaj, no prowjerjaj.*"
-- Russian Proverb

13

Thank you for your attention!

Walter.Fumy@bdr.de