

Living in the panopticon

Denis A Nicole

2013-10-23



PANOPTICON;
OR
THE INSPECTION-HOUSE:

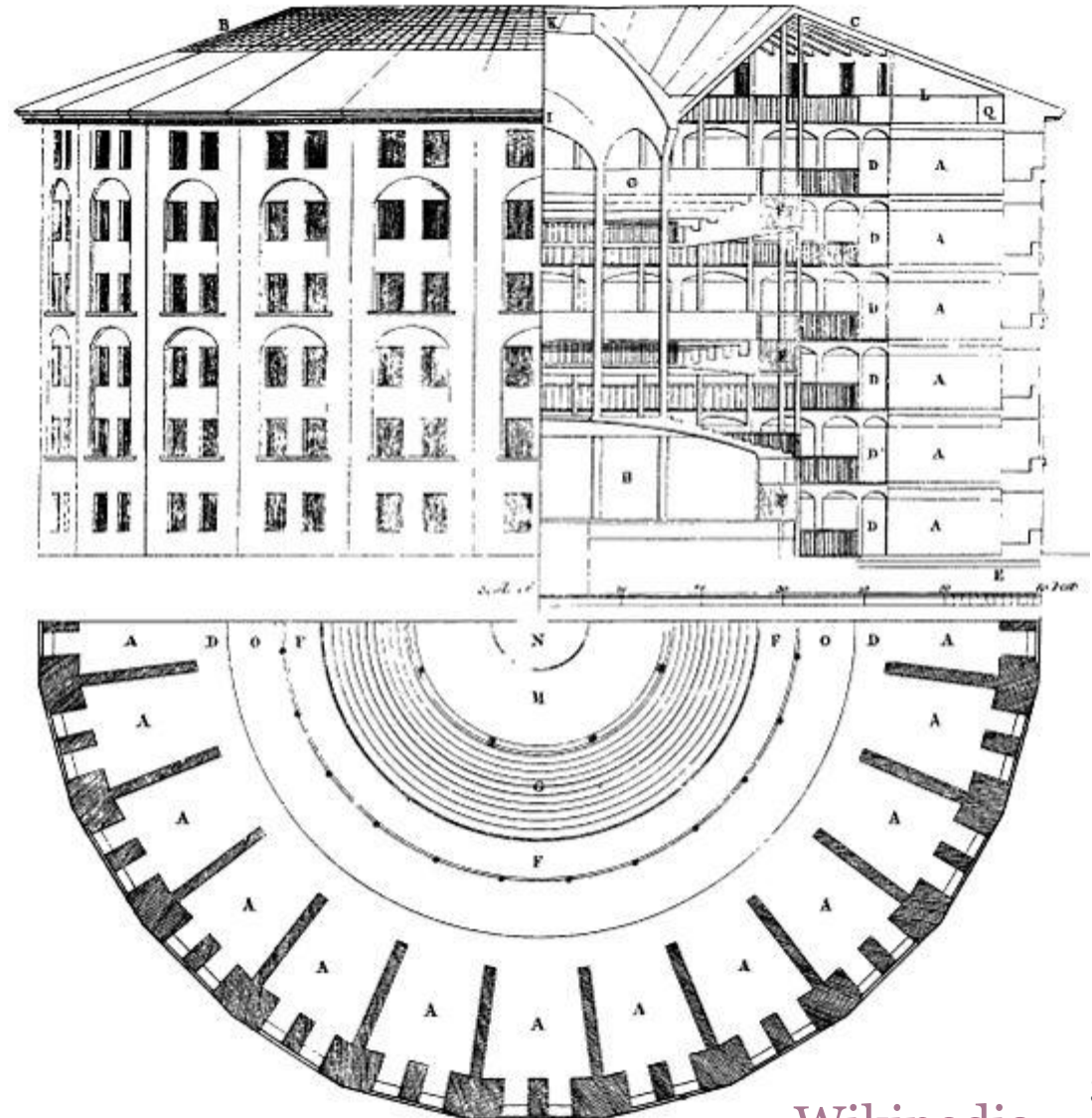
CONTAINING THE
IDEA OF A NEW PRINCIPLE OF CONSTRUCTION
APPLICABLE TO
ANY SORT OF ESTABLISHMENT, IN WHICH PERSONS OF
ANY DESCRIPTION ARE TO BE KEPT UNDER INSPECTION;

AND IN PARTICULAR TO
PENITENTIARY-HOUSES,
PRISONS, HOUSES OF INDUSTRY, WORK-HOUSES, POOR-HOUSES, LAZARETTOS, MANUFACTORIES, HOSPITALS, MAD-HOUSES, AND SCHOOLS:
WITH

A PLAN OF MANAGEMENT
ADAPTED TO THE PRINCIPLE:
IN A SERIES OF LETTERS,
WRITTEN IN THE YEAR 1787, FROM CRECHEFF IN WHITE
RUSSIA. TO A FRIEND IN ENGLAND

BY JEREMY BENTHAM,
OF LINCOLN'S INN, ESQUIRE.

The design



It was built—in Cuba



Presidio Modelo



He still works at UCL



Is (hidden) surveillance *of itself* a problem?

- The architecture incorporates a tower central to a circular building that is divided into cells, each cell extending the entire thickness of the building to allow inner and outer windows. The occupants of the cells are thus backlit, isolated from one another by walls, and subject to scrutiny both collectively and individually by an observer in the tower who remains unseen. Toward this end, Bentham envisioned not only venetian blinds on the tower observation ports but also maze-like connections among tower rooms to avoid glints of light or noise that might betray the presence of an observer.

A new mode of obtaining power of mind over mind, in a quantity hitherto without example.

A mill for grinding rogues honest.

Bentham, Jeremy *The Panopticon Writings*. Ed. Miran Bozovic (1995)
Semple, Janet (1993). *Bentham's Prison: a Study of the Panopticon Penitentiary*.

Why should we worry?

- The reality is that the British public are well aware that its intelligence agencies have neither the time nor the remotest interest in the emails or telephone conversations of well over 99% of the population who are neither potential terrorists nor serious criminals. Modern computer technologies do permit the separation of those that are of interest from the vast majority that are not.
- Our system is not perfect. There are occasions when the intelligence obtained may be of such little value as not to justify the diminution in privacy associated with obtaining it.
- But I have yet to hear of any other country, either democratic or authoritarian, that has both significant intelligence agencies and a more effective and extensive system of independent oversight than the UK and the US.

Rt Hon Sir Malcolm Rifkind
Chair, Intelligence and Security Committee
20th September 2013



Intelligence Services Act 1994

3.—(1) There shall continue to be a Government Communications Headquarters under the authority of the Secretary of State; and, subject to subsection (2) below, its functions shall be—

(a) to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material; and

(b) to provide advice and assistance about—

(i) languages, including terminology used for technical

(ii) cryptography and other matters relating to the protection of information and other material,

to the armed forces of the Crown, to Her Majesty's Government in the United Kingdom or to a Northern Ireland Department or to any other organisation which is determined for the purposes of this section in such manner as may be specified by the Prime Minister.

(2) The functions referred to in subsection (1)(a) above shall be exercisable only—

(a) in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or

(b) in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands; or

(c) in support of the prevention or detection of serious crime.

All's fair in trade negotiations.

No strike-breaking.

Economic interests

- ...are very widely drawn.
- Spying on the EU is legal.



Markus Kuhn has a good account of DROPMIRE as a TEMPEST attack. The day I gave this talk, Le Monde revealed that DROPMIRE is a *passive* attack; apparently nothing was done to the FAX itself to increase its emanations.

Give our negotiators confidence

- Learn their opposite numbers' strategy.
- Tittle-tattle gives ministers a warm feeling of control.
- Can they resist the temptation to treat domestic politics the same way?
- Is there an inevitable drift to corrupt domestic surveillance?

Priorities?

Scotland Yard spied on critics of police corruption

Exclusive: undercover officers in Special Demonstration Squad targeted political campaigns against Metropolitan police

 Follow Paul Lewis by email **BETA**

Rob Evans and **Paul Lewis**

The Guardian, Monday 24 June 2013 21.14 BST



Mark Jenner, the undercover officer in the Metropolitan police's special demonstration squad, who spied on the Colin Roach Centre

Scotland Yard deployed undercover officers in political groups that sought to uncover corruption in the Metropolitan [police](#) and campaigned for justice for people who had died in custody, the Guardian can reveal.

And they are real people

MailOnline

NSA employees used phone tapping tools to spy on their girlfriends and 'cheating' husbands

- Investigation into abuses of power at the NSA shows that at least a dozen employees tracked their romantic interests phone calls and emails
- One female employee admitted to looking into her husband's call logs after seeing an unknown foreign number on his cell
- Some have resulted in demotions and the Justice Department is investigating but none of the cases have been prosecuted

By [MEGHAN KENEALLY](#)

PUBLISHED: 14:15, 27 September 2013 | UPDATED: 14:16, 27 September 2013

...who might misbehave

MailOnline**Immigration officer fired after putting wife on list of terrorists to stop her flying home**

By STEVE DOUGHTY

UPDATED: 18:11, 30 January 2011



0 View comments

An immigration officer tried to rid himself of his wife by adding her name to a list of terrorist suspects.

He used his access to security databases to include his wife on a watch list of people banned from boarding flights into Britain because their presence in the country is 'not conducive to the public good'.

As a result the woman was unable for three years to return from Pakistan after travelling to the county to visit family.

The tampering went undetected until the immigration officer was selected for promotion and his wife name was found on the suspects' list during a vetting inquiry.



How many more?

- We only found out about Snowden because *he told us*.
- How many more?
 - for money,
 - for ideology,
 - from blackmail,
 - from sickness.

Not just the *five eyes*

TOP SECRET//COMINT//REL TO USA, ISR

(TS//SI//REL) MEMORANDUM OF UNDERSTANDING (MOU)
BETWEEN THE
NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE (NSA/CSS)
AND
THE ISRAELI SIGINT NATIONAL UNIT (ISNU)
PERTAINING TO THE PROTECTION OF U.S. PERSONS

I. (U) PURPOSE

- a. (TS//SI//REL) This agreement between NSA and The Israeli SIGINT National Unit (ISNU) prescribes procedures and responsibilities for ensuring that ISNU handling of materials provided by NSA – including, but not limited to, Signals Intelligence (SIGINT) technology and equipment and raw SIGINT data (i.e., signals intelligence information that has not been reviewed for foreign intelligence purposes or minimized) – is consistent with the requirements placed upon NSA by U.S. law and Executive Order to establish safeguards protecting the rights of U.S. persons under the Fourth Amendment to the United States Constitution.
- b. (TS//SI//REL) This agreement will apply to any SIGINT raw traffic, technology, or enabling that NSA may provide to ISNU. This agreement applies only to materials provided by NSA and shall not be construed to apply to materials collected independently by ISNU.



Does it *blowback* into domestic politics?



<http://www.aipac.org/>

Once upon a time

...we suspected IBM and the NSA of weakening an important cipher: DES.

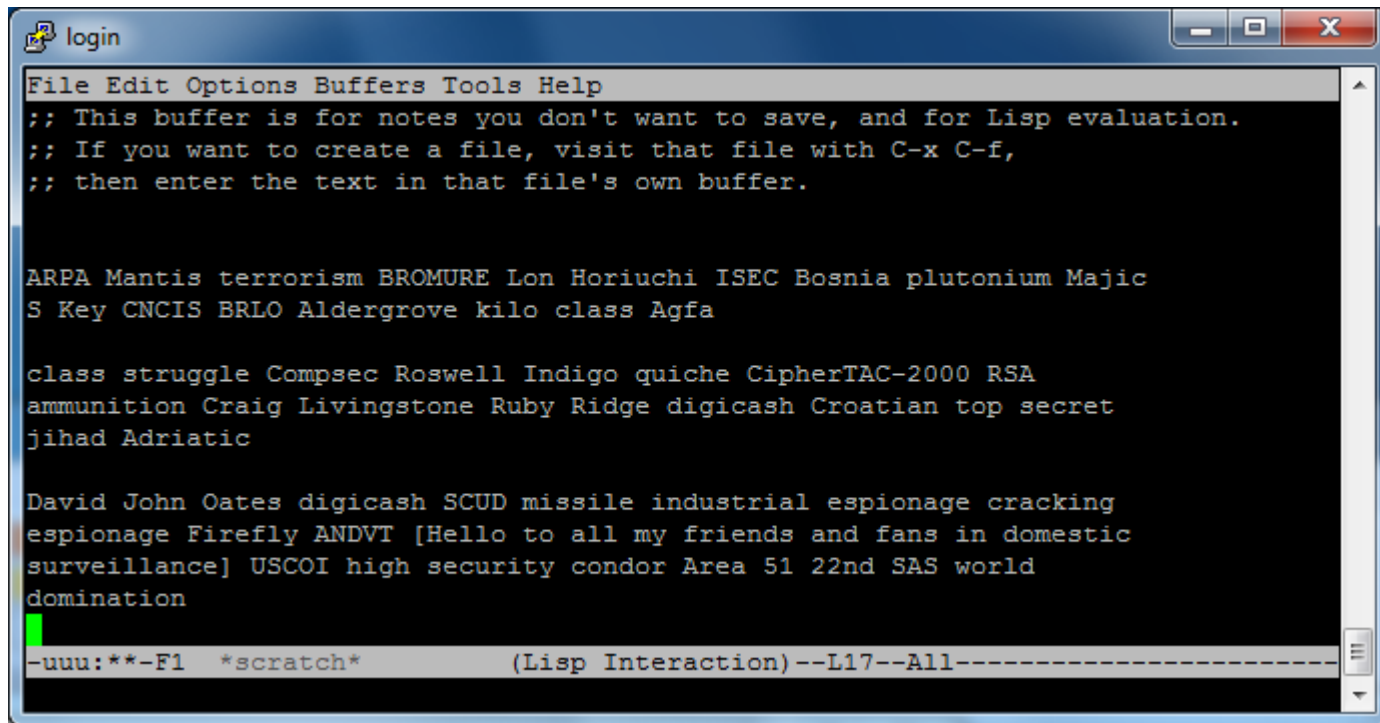
But it turned out they had used their secret knowledge to **strengthen** its resistance to *differential cryptanalysis*.

- <http://www.cs.haifa.ac.il/~orrd/BlockCipherSeminar/Lecture2-Differential.pdf>
- <http://simson.net/ref/1994/coppersmith94.pdf>

Times have changed...

We used to poke fun at surveillance

- emacs META-X spook



```
login
File Edit Options Buffers Tools Help
;; This buffer is for notes you don't want to save, and for Lisp evaluation.
;; If you want to create a file, visit that file with C-x C-f,
;; then enter the text in that file's own buffer.

ARPA Mantis terrorism BROMURE Lon Horiuchi ISEC Bosnia plutonium Majic
S Key CNCIS BRLO Aldergrove kilo class Agfa

class struggle Compsec Roswell Indigo quiche CiphertAC-2000 RSA
ammunition Craig Livingstone Ruby Ridge digicash Croatian top secret
jihad Adriatic

David John Oates digicash SCUD missile industrial espionage cracking
espionage Firefly ANDVT [Hello to all my friends and fans in domestic
surveillance] USCOI high security condor Area 51 22nd SAS world
domination

-uuu:**-F1 *scratch* (Lisp Interaction)--L17--All-----
```

Steve Strassman went on to build the cloud at VMWare

```
;; Spook phrase utility
;; Copyright (C) 1988 Free Software Foundation
;; This file is part of GNU Emacs.
;; GNU Emacs is free software; you can redistribute it and/or modify
;; it under the terms of the GNU General Public License as published by
;; the Free Software Foundation; either version 1, or (at your option)
;; any later version.

; Steve Strassmann (straz@media-lab.media.mit.edu) didn't write
; this, and even if he did, he really didn't mean for you to use it
; in an anarchistic way.; May 1987; To use this:

; Just before sending mail, do M-x spook.
; A number of phrases will be inserted into your buffer, to help
; give your message that extra bit of attractiveness for automated
; keyword scanners.
```

There's also a story about John Bridle and the JSRU

http://amhistory.si.edu/archives/speechsynthesis/ss_jsru.htm

And we had fun with NSAKEY

Send a secret message to the NSA (1999):

```
Type Bits/KeyID      Date           User ID
pub  1024/51682D1F 1999/09/06 NSA's Microsoft CAPI key <postmaster@nsa.gov>
```

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: 2.6.3i

```
mQCPAzfTdH0AAAEALqOFF7jzRYPtHz5PitNhCYVryPwZZJk2B7cNaJ9OqRQiQoi
e1YdpAH/OQh3HSQ/butPnjUZdukPB/0izQmczXHoW5f1Q5rbFy0y1xy2bCbFsYij
4ReQ7QHrMb8nvGZ7OW/YKDCX2LOGnMdRGjSW6CmjK7rW0veqfoypgF1RaC0fABEB
AAG0LU5TQSDzIE1pY3Jvc29mdCBDQVBjIGtleSA8cG9zdG1hc3RlckBuc2EuZ292
PokBFQMFEDfTdJE+e8qoKLJFUQEBHnsH/ihUe7oq6DhU1dJjvXWcYw6p1iW+0euR
YfZjwpzPotQ8m5rC7FrJDUbgqQjoFDr++zN9kD9bjNPVUx/ZjCvSFTNu/5X1qn1r
it7IHU/6Aem1h4Bs6KE5MPpjKRxRkqQjbW4f0cgXg6+LV+V9cNMy1ZHRef3PZCQa
5DOI5crQ0IWyjQct9br07BL9C3X5WHNNRsRIr9WiVfPK8eyxhNYl/NiH2GzXYbNe
UWjaS2KuJNVvozjxGymcnNTwJltZK4RLZxo05FW2InJbtEfMc+m823vVltm9l/f+
n2iYBAaDs6I/0v2AcVKNy19Cjncc3wQZkaiIYqfPZL19kT8vDNGi9uE=
=PhHT
```

-----END PGP PUBLIC KEY BLOCK-----

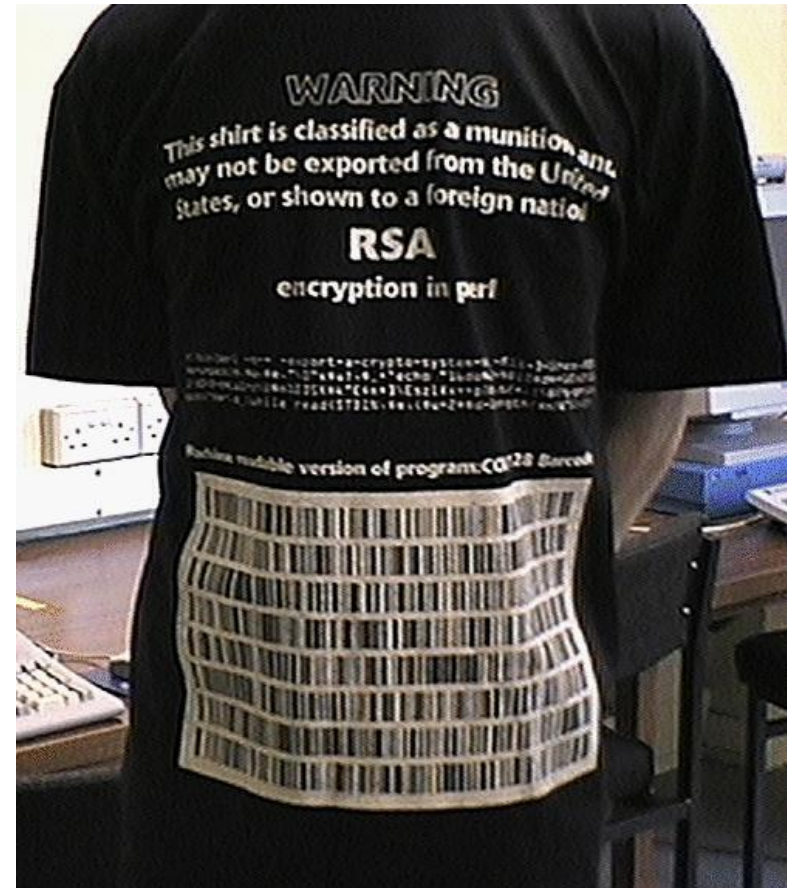
The trouble has been brewing a while

- The crypto wars: Clipper and key escrow

<http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html?pagewanted=all&src=pm>
<http://www.crypto.com/papers/eesproto.pdf>

- Export controls

<http://www.cypherspace.org/adam/uk-shirt.html>



The community thought it had won

The Crypto Wars Are Over!

RELEASE TIME: 00.01, 25 May 2005

The "crypto wars" are finally over - and we've won!

On 25th May 2005, Part I of the Electronic Communications Act 2000 will be torn out of the statute book and shredded, finally removing the risk of the UK Government taking powers to regulate companies selling encryption services.

The crypto wars started in the 1970s when the US government started treating cryptographic algorithms and software as munitions and interfering with university research in cryptography. In the early 1990s, the Clinton administration tried to get industry to adopt the Clipper chip - an encryption chip for which the government had a back-door key. When this failed, they tried to introduce key escrow - a policy that all encryption systems should leave a spare key with a 'trusted third party' that would hand the key over to the FBI on demand. They tried to crack down on encryption products that did not contain key escrow. When software developer Phil Zimmermann developed PGP, a free mass-market encryption product for emails and files, the US government even started to prosecute him, because someone had exported his software from the USA without government permission.

In its dying days, John Major's Conservative Government proposed draconian controls in the UK too. Any provider of encryption services would have to be licensed and encryption keys would have to be placed in escrow just in case the Government wanted to read your email. New Labour opposed crypto controls in opposition, which got them a lot of support from the IT and civil liberties communities. They changed their minds, though, after they came to power in May 1997 and the US government lobbied them.

However, encryption was rapidly becoming an important technology for commercial use of the Internet - and the new industry was deeply opposed to any bureaucracy which prevented them from innovating and imposed unnecessary costs. So was the banking industry, which worried about threats to payment systems from corrupt officials. In 1998, the Foundation for Information Policy Research was established by cryptographers, lawyers, academics and civil liberty groups, with industry support, and helped campaign for digital freedoms.

<http://www.fipr.org/press/050525crypto.html>

What (and who) can we trust?

Denis A Nicole

2013-10-23

Who do we fear?

- Terrorists? (yes: and I'm willing to do my best to help)
- Criminals (yes: and I'm willing to do my best to help)
- International competitors? (not me, at the moment)
- Corrupt government employees? (yes)
- Moderately corrupt government—mission creep (yes: I'm in a Union)
- Seriously corrupt government (no, not in the UK)
- Honest policing (not me) But the *five eyes* have suppressed alcohol, sexual orientation, run the War on Drugs.

Who do we trust?

I'm generally happy with the work of UK and US academic cryptographers and analysts, particularly those who have felt free to be openly critical of government. For example:

- The Security Group at Cambridge.
- The Information Security Group at Royal Holloway.
- The Cryptography Group at Bristol.
- Daniel Bernstein
- Bruce Schneier
- Matthew Green
- Ed Felten

What's broken?

- PRNGs (be really afraid)
- GSM
- Microsoft (_NSAKEY, Skype...)
- VPNs (MSCHAP v2)
- Intel (microcode updates, rdrand, vPRO, AMT)
- PKI (all the CAs and most of the server keys?)
- Cisco, Huawei (probably)
- RC4, RC4 key scheduling

PRNG/RNGs

- The spook's first choice.
- Most crypto relies on random numbers, e.g for session keys.
- Very easy to corrupt:
 - Reduce the number space:
 - Debian `openssl 0.9.8c-1`
 - Embedded hosts can be a problem.
 - Find shared factors in modulus
 - Leak state
 - TrueCrypt on Windows?


```
int getRandomNumber()  
{  
    return 4; // chosen by fair dice roll.  
              // guaranteed to be random.  
}
```

DEBIAN

GUARANTEED ENTROPY.

The author of the change continues to work with Debian

Ron was wrong, Whit is right

Arjen K. Lenstra et al.

We checked the computational properties of millions of public keys that we collected on the web. The majority does not seem to suffer from obvious weaknesses and can be expected to provide the expected level of security. We found that on the order of 0.003% of public keys is incorrect, which does not seem to be unacceptable. We were surprised, however, by the extent to which public keys are shared among unrelated parties. For ElGamal and DSA sharing is rare, but for RSA the frequency of sharing may be a cause for concern. What surprised us most is that many thousands of 1024-bit RSA moduli, including thousands that are contained in still-valid X.509 certificates, offer no security at all. This may indicate that proper seeding of random number generators is still a problematic issue.

<http://eprint.iacr.org/2012/064.pdf>

See also the Taiwan smart card problems

<http://smartfacts.cr.yp.to/smartfacts-20130916.pdf>



THE RESOURCE FOR SECURITY EXECUTIVES

Google™ Custom Search



News

Tools & Templates ▾

Reviews

eThreatz

Blogs

Directory

Galleries

Events

CSO Team

Industries ▾

Data Protection ▾

Identity & Access ▾

Mobile Security

Security Leadership ▾

Risk Management



Targeted analytics deliver better web security



Malware risk is not what's keeping
Australians from online banking,
shopping, ACMA



The Security Odyssey



Red vs Blue – the security response
war room

TrueCrypt audit fundraiser cracks \$34K

Liam Tung (CSO Online (Australia)) — 18 October, 2013 10:03

Security experts who are crowd-funding a project to probe the file and disk encryption tool TrueCrypt for backdoors look set to reach their financial target.

The project "Is TrueCrypt Audited Yet?" launched on Monday and will attempt to put to rest lingering concerns over the popular encryption software with a public audit of the Windows, Linux and Mac OS X versions of TrueCrypt.

CSO Corporate
Partners



Get exclusive
access to CSO,
invitation only events,
reports & analysis.
Sign up now »

Username

OR

Sign in »

RELATED STORIES

On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng

Dan Shumow
Niels Ferguson
Microsoft

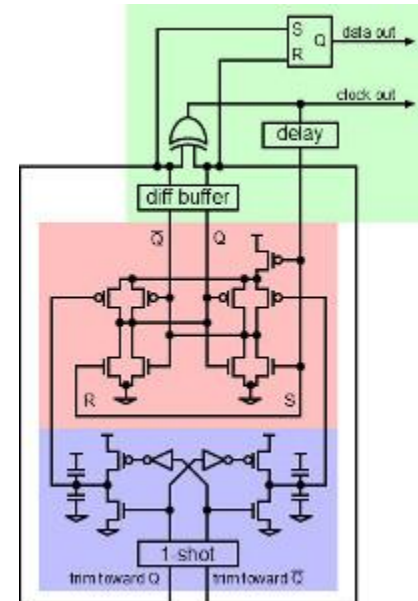
http://www.wired.com/politics/security/commentary/securitymatters/2007/11/securitymatters_1115

Ivy Bridge RNG

- The output of the ES is fairly high-quality, but it isn't strong enough for cryptographic purposes. The output won't be entirely balanced. The feedback circuit introduces bias, and the entire circuit may be influenced by analogue effects such as ringing. To solve this, the output is passed through a cryptographic conditioner, which condenses many mediocre random bits into a few very good ones. Even "unhealthy" samples are sent to the conditioner, because they can't hurt the quality of its output.
- The conditioner produces a 256-bit seed value every few microseconds. But if all the cores on the chip are asking for random data, this won't satisfy the demand. Therefore, the seed value is fed into a NIST SP800-90A-based pseudorandom generator. This generator uses 128-bit AES in counter mode, and increases the amount of data that the generator can produce to around 800 megabytes per second.

<http://electronicdesign.com/learning-resources/understanding-intels-ivy-bridge-random-number-generator#1>

- But: can you test the implementation?
- And, it can be subverted by “updated” microcode.



A nasty idea

- **xor** is not very common in mixed C code. So, say a system (Linux) was using **rand** just to improve an existing RNG by **xoring** the output with **rand**.
- So the NSA/GCHQ would subvert this system by replacing the **xor** with a **mov**, so only the **rand** output was used.
- You'd do that by sending a microcode update which causes **rand** to:
 1. return a predictable value, and
 2. stuff that value in as the result of the *next* **xor** operation.

While we're on Intel...

- There are potential very late attacks on the RNG hardware.
- There is a new, allegedly raw-er Intel RNG stream: rdseed
- What do you know about vPro?
- What is AMT doing with *your* laptop.
- You can hide malware in any programmable component:
 - BIOS
 - Disk controller
 - Network interface
 - FPGA

PKI

- One way or another, assume NSA/GCHQ/*Central Committee of the Communist Party of China* have all the server X509 keys: cooperation, National Security Letters, theft.
- So, if they really care, they *can* run MITM attacks on all **https:** traffic.
- But...their Narus (BAe?) boxes are packed with FPGAs for *Deep Packet Inspection*. I don't believe they can maintain enough state to MITM all the **https:** traffic.
- I doubt they can even decode (with the keys) anything more complex than RC4.

So my guess is...

- If your TLS uses RC4 without forward secrecy, and NSA/GCHQ have any interest in the traffic, they can read it in bulk in real time on their DPI kit.
- If you use AES or DES without forward secrecy, they can read your traffic with a bit of effort, possibly not in real time.
- If you use forward secrecy, it becomes expensive for them. They have to maintain a continuous MITM; they'd need to really care.

If you care

- Don't use Windows. Don't use much of Linux.
- Use 2048-bit RSA. And avoid an exponent of 3.
- Avoid Elliptic Curves. They keep bad company.
Except this one: Curve25517
- Use Diffie–Hellman key exchange for *forward secrecy*. But be *very careful* with your PRNG.
- Finally, we need a symmetric cipher. Avoid RC4. There are known issues, and we've been herded there by someone.

Block cipher support is tricky right now

- AES is probably fine itself.
- But you need the right *mode*; there are issues with CBC schemes. The latest attack is Lucky13.
- If your system will support it, use AES-GCM.
- Something like:
`TLS_DH_RSA_WITH_AES_256_GCM_SHA384`
- Which reminds me...
Possibly bad things are happening to SHA3.

Attacks on the Linux kernel (2003)

- “They” do “try it on”

```
wait4()
```

```
if ((options == (__WCLONE|__WALL)) && (current->uid = 0))  
    retval = -EINVAL;
```

Bruce Schneier is too trusting

He says:

“Install the minimum software set you need to do your job, and disable all operating system services that you won't need. The less software you install, the less an attacker has available to exploit.

I downloaded and installed OpenOffice, a PDF reader, a text editor, TrueCrypt, and BleachBit. That's all.”

Lets look at that list

- OpenOffice: there's a lot here. Can't he make do with vim? Or gedit. To much bloat and history to trust.
- A PDF reader: surely not Acrobat, a big attack surface.
- TrueCrypt: has anonymous authors and the Windows version pads output with unexplained data. And does not seem to build exactly from source.

GSM

- There has been publicity about secret US government orders to allow tapping of cellular telephone messages, mainly to collect metadata.
- That's sad; any decent SIGINT service should be able to manage with their own resources, not have to ask.
<http://www.washingtontimes.com/news/2013/mar/29/feds-fbi-warrantless-cell-tracking-very-common/>
- There seems to be a recurring problem; traditional *bugging* techniques cannot affordably handle the large volume of data NSA/GCHQ think they need, so they have to go to the suppliers. And they don't want to reveal their targets, so they have to sweep up even more data.
- Furthermore, they can't afford (Skynet: PPP) high bandwidth international links, so have to leave data in situ.
- It seems News International mainly just used default passwords on voicemail; we can do much better.

GSM Security

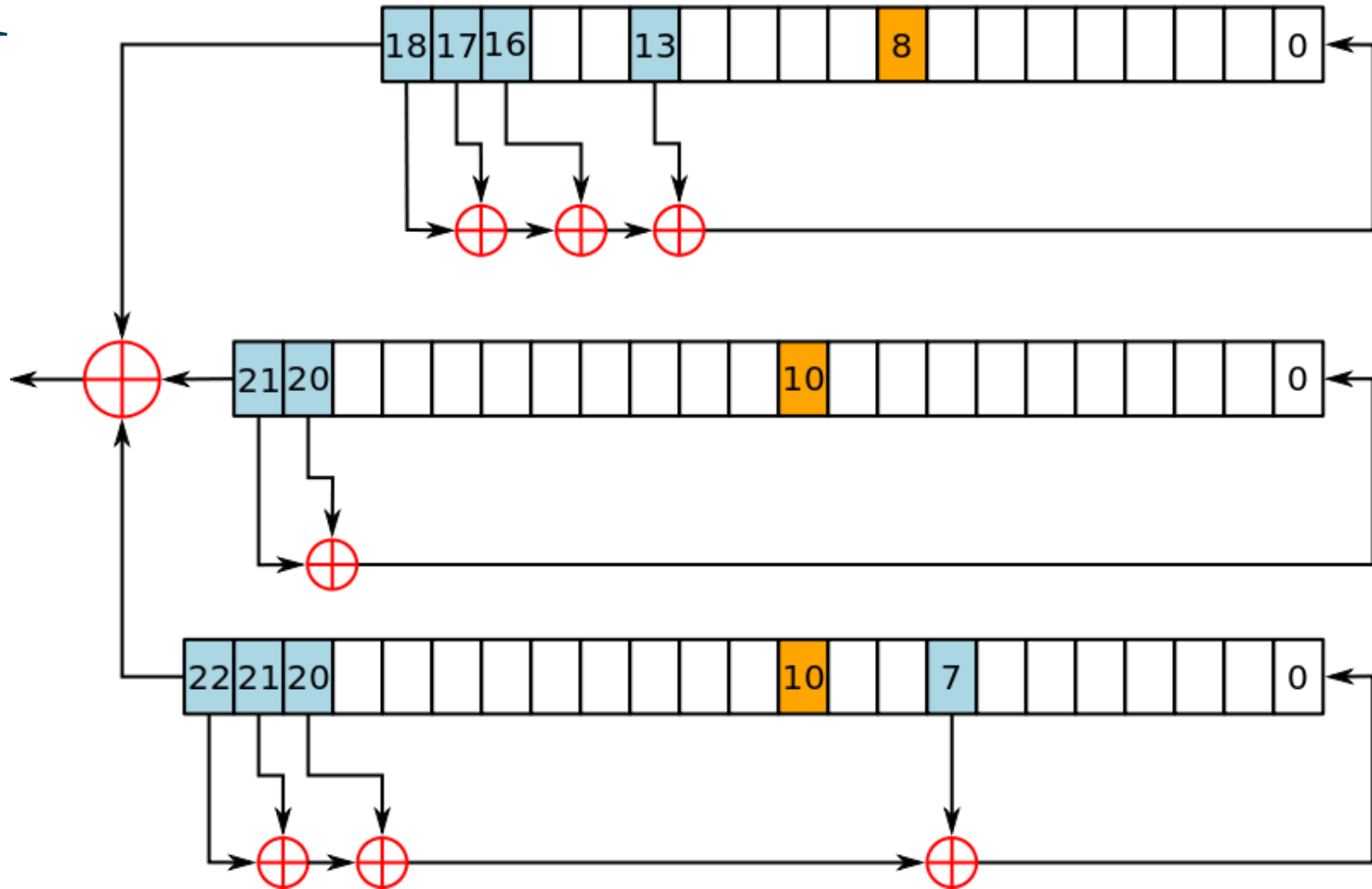
The original A5 series of stream ciphers operate on 114 bit frames. Yes, I did say stream.

- A5/0: No encryption. Used, it seems, in India to reduce costs. You only get a *no-encryption* warning if both handset and network turn it on.

<http://itsecuritypro.co.uk/morestories/indian-gsm-networks-using-little-or-no-encryption/>

- A5/1: Stream cipher, based on LFSR. Standard on 2G.
- A5/2: Weakened A5/1, mainly for export but still used in US in 2006. Now out of use.
- A5/3: Block cipher (Kasumi). Weakened version of MISTY.

A5/1



LFSR clocks if it's yellow bit is in the majority

http://en.wikipedia.org/wiki/File:A5-1_GSM_cipher.svg

A5/1 Easily broken on-air (2010)

Even reprogrammed cheap phones can intercept hopping calls



Start with a EUR 10 phone from 2006

Upgrade to an open source firmware

Patch DSP code to ignore encryption

Add faster USB cable

Remove uplink filter

You get:

Debugger for your own calls

Single timeslot sniffer

Multi timeslot sniffer

Uplink + downlink sniffer

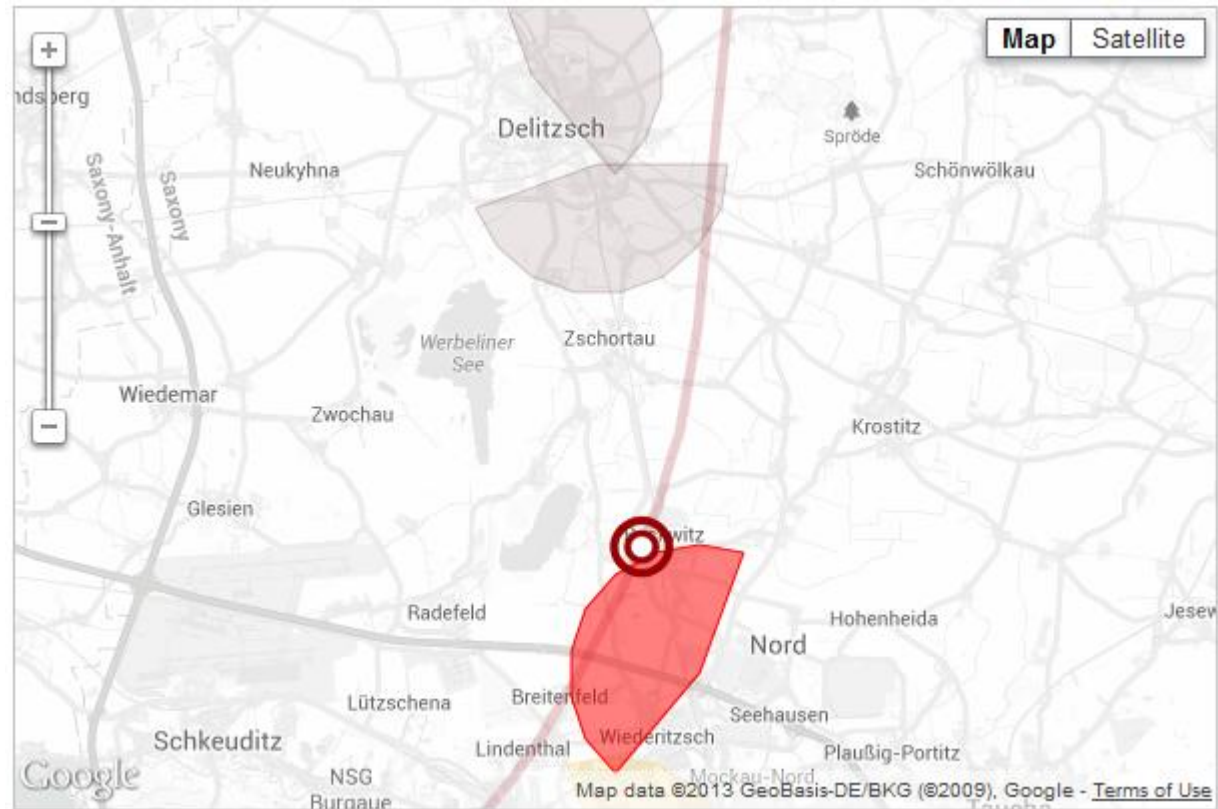
Demo

 SECURITYRESEARCHLABS

A5/3

- A5/3 is a Feistel network block cipher, similar to DES.
- Attack the encryption: A5/3 is weaker than MISTY.
<http://eprint.iacr.org/2010/013.pdf>
- The practical approach, attack the protocol: a5/1 and a5/3 use the same key.
<http://www.cs.technion.ac.il/users/wwwb/cgi-bin/tr-get.cgi/2006/CS/CS-2006-07.pdf>

Tracking



And, of course, tracking by networks, with data retained for law enforcement use, is routine.

<http://www.zeit.de/datenschutz/malte-spitz-data-retention>