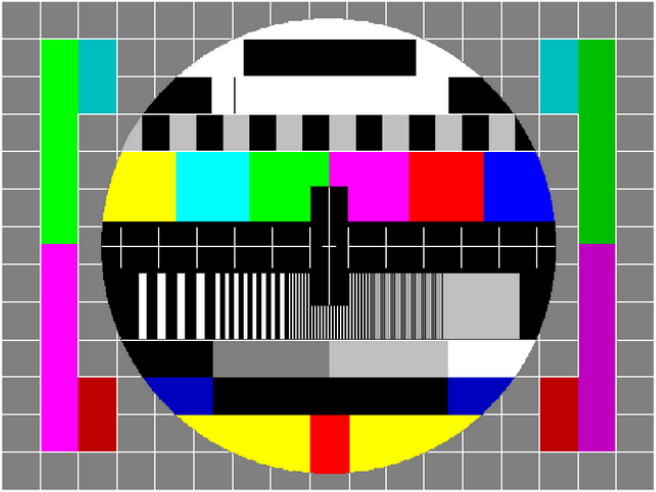


Post Snowden Security

Stefan Marsiske, <s@ctrlc.hu>

September 26, 2013

Adversaries. . .

“[. . .] show an alarming trend for the state to view everyday people as adversaries.” - C. Doctorow

. . . Adversaries

- “Civilian”
- Criminal
- Industrial
- Totalitarian

Psyops^H^H^Hchology

Civilian reaction

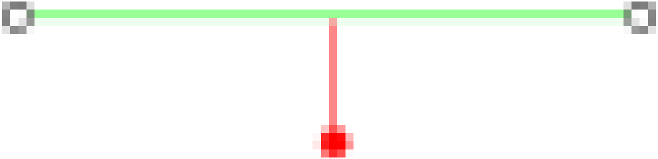
- cryptoparties
- cryptocats
- W3C web crypto
- smartphone crypto

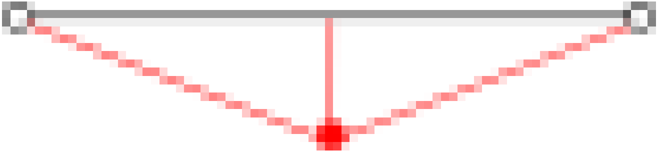
Jon Callas. . .

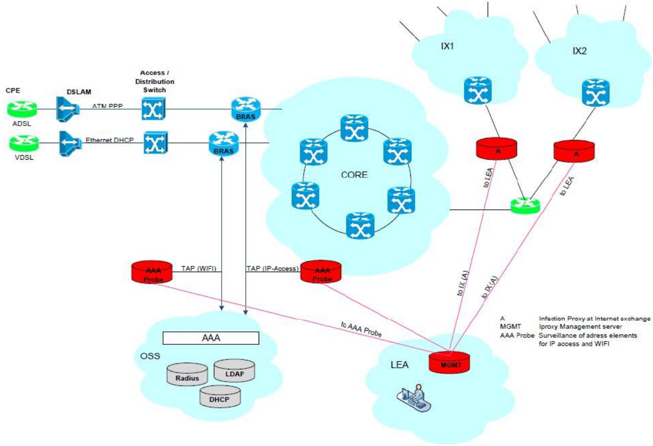
> *“one of my bugaboos about security is something I call ”security arrogance.“ Security arrogance is when the security person tells the users what their threat model should be. It’s closely related to another thing I talked about a decade ago that I called ”the security cliff“—you start with no security and to get to security, you have to climb a cliff rather than ascend a ramp in that you can’t stop halfway up. I believe that one of the ways we security people shoot our clients in the foot is to focus on the ways that security is imperfect and thus argue that less-than-perfect security is worse than no security.”*

False sense of security

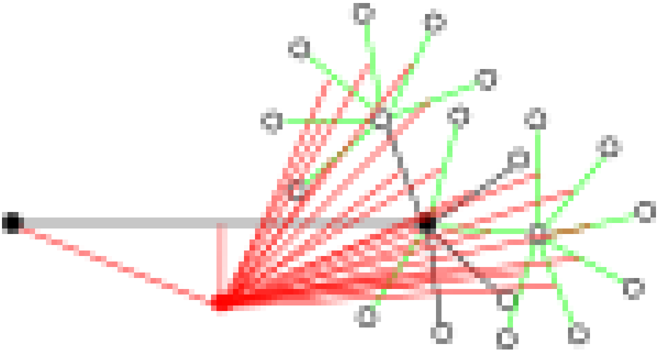
Against unforgetting, lawful, hyper-resourceful adversary

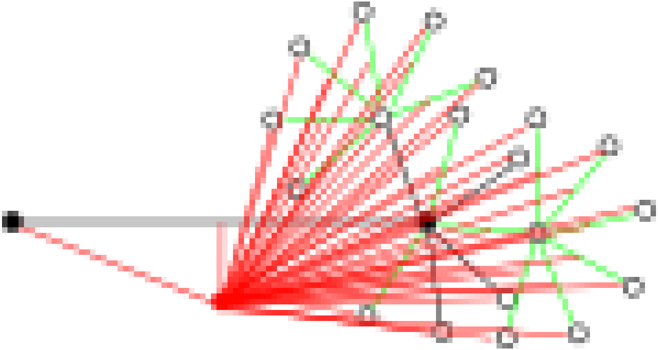




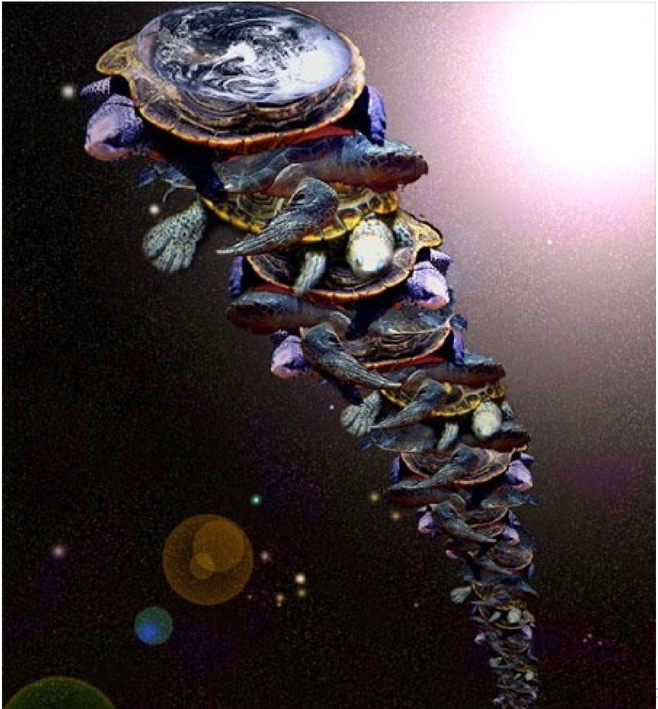


A	Infection Proxy at Internet exchange
MGMT	Iproxy Management server
AAA Probe	Surveillance of adress elements for IP access and WIFI





would you want to have surgery over the internet?



Security

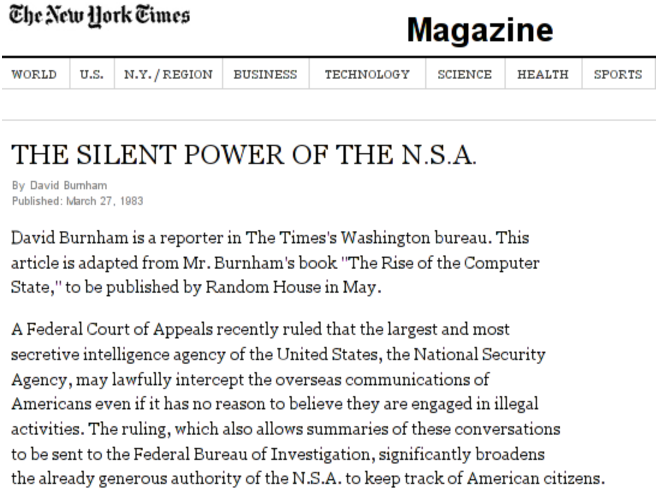
- physical, psychological security
- threat analysis/modelling
- trade-off - hygiene
- Free OS
- Free HW

Mindset

- question everything
- it's a process
- there's no 100%
- the attacker only has to succeed once, the defender always - expect to be owned sooner or later

internet-sea.mp4

History



THE SILENT POWER OF THE N.S.A.

By David Burnham
Published: March 27, 1983

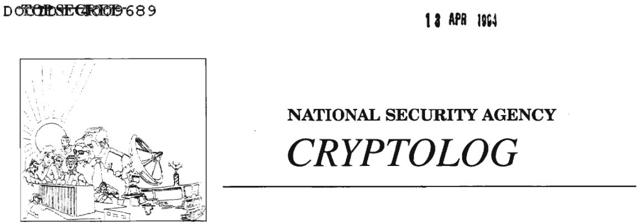
David Burnham is a reporter in The Times's Washington bureau. This article is adapted from Mr. Burnham's book "The Rise of the Computer State," to be published by Random House in May.

A Federal Court of Appeals recently ruled that the largest and most secretive intelligence agency of the United States, the National Security Agency, may lawfully intercept the overseas communications of Americans even if it has no reason to believe they are engaged in illegal activities. The ruling, which also allows summaries of these conversations to be sent to the Federal Bureau of Investigation, significantly broadens the already generous authority of the N.S.A. to keep track of American citizens.

History

(U) Three of the last four sessions were of no value whatever, and indeed there was almost nothing at Euroc- rypt to interest us (this is good news!). The scholarship was actually extremely good; it's just that the directions which external cryptologic researchers have taken are remarkably far from our own lines of interest.

History



DOCID: 4009689

~~TOP SECRET~~

13 APR 1964

NATIONAL SECURITY AGENCY

CRYPTOLOG

History

Thursday morning: digital signatures and electronic cash, complexity theory and cryptography II.

History

(U) There were no proposals of cryptosystems, no novel cryptanalysis of old designs, even very little on hardware design. I really don't see how things could have been any better for our purposes. We can hope that the absentee cryptologists stayed away because they had no new ideas, or even that they've taken an interest in other areas of research.

implementations.mp4

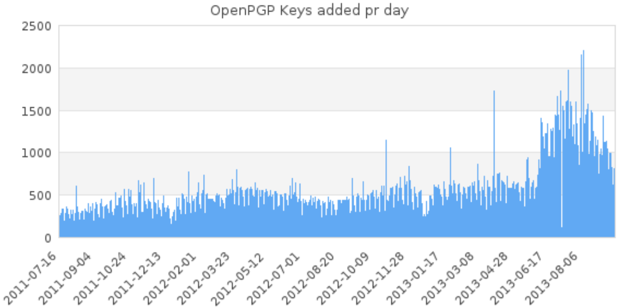
Crypto AGs

- Windows
- Lotus Notes
- ipsec
- Openbsd
- SSL
- GSM
- RSA
- Hushmail
- Google

SSL

- Padding Oracle (2002, 2006)
- Renegotiation Attack (2009)
- BEAST (2011, TLSv1.1)
- CRIME (2012, TLS compression off)
- BREACH (2013,)
- Lucky 13 (2013,)
- RC4 (2013,)

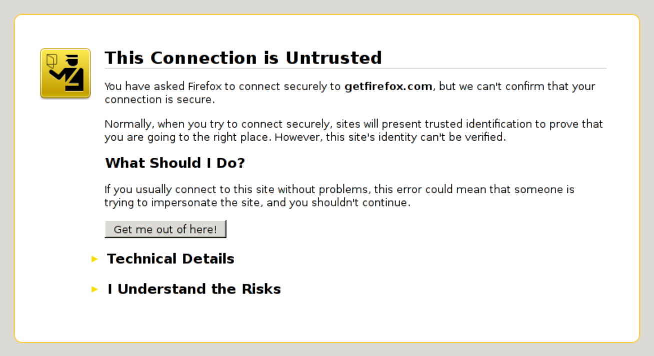
PGP



- easily fingerprintable (DPI, forensics)
- no PFS
  - `http://tools.ietf.org/html/draft-brown-pgp-pfs-01`
  - steed
- no AE in symmetric
- still no ECC

Firefox

- compartmentalization
- tls1.2 support
- signed builds `http://releases.mozilla.org/pub/mozilla.org/firefox/releases/latest/`



This Connection is Untrusted

You have asked Firefox to connect securely to **getfirefox.com**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

OTR apps

- jitsi
- pidgin

ZRTP apps

keymanagement

- rngs
- ephemerals
- lifecycle
- deletion
- access
- size
- reverse engineer

algos.mp4

RNGS

- Dual_EC_DRBG (2007,)
- /dev/random is good - if seeded
- backdooring, running a symmetric cipher in counter mode, with known counter
- CSRNG
- 8d16, deck of cards
- haveged

HW entropy sources

- `http://www.entropykey.co.uk/`
- atmospheric noise from radio
- reverse PNL junctions, timing electron jumps.
- Timing radioactive decay using Americium-241
- `http://www.fourmilab.ch/hotbits/hardware3.html`
- Opening up the CCD on a web camera fully in a completely dark box.
- Termal noise from resistors.
- Clock drift from quartz-based clocks and power fluctuations.

(U) The allegation (almost certainly correct) that certain public-key systems might be implemented more securely by using elliptic curves has produced the pre- dictable spate of papers on elliptic curves. We were for- tunate to have only two such talks on the current agenda.

ECC

$$x^2 + y^2 = c^2(1 + dx^2y^2)$$

$$By^2 = x^3 + Ax^2 + x$$

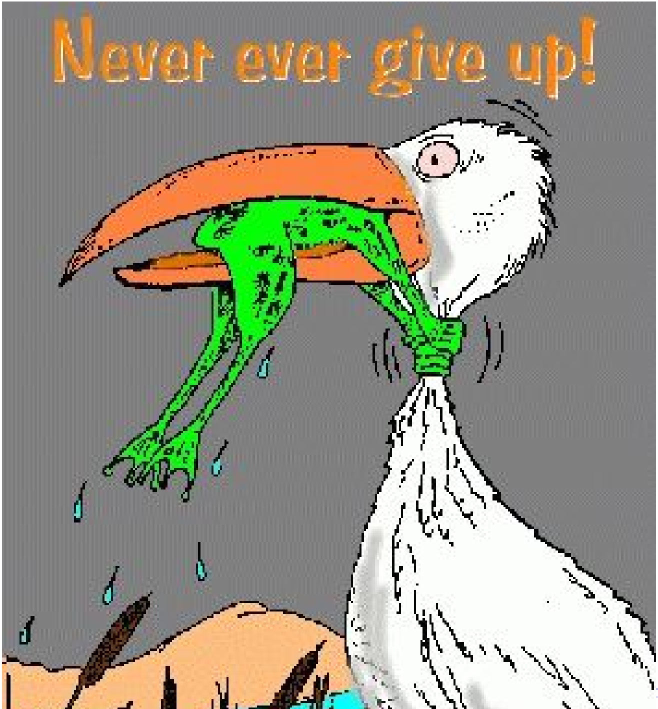
- NIST - Montgomery, Edwards nada - hard to implement
- identifiable points
- crypto constants
- kleptography

Crypto building blocks

- AE (AEAD)
- PFS
- CSRNG
- PAKE
- SRP/augmented EKE
- Scrypt/PBKDF2
- Zero Knowledge systems (freecoin, Brands)
- Multiparty calculations

Post-Quantum

- Cramer-Shoup QR/DCR
- Code-based: McEliece (1978), Niederreiter (1986), McBits (2013)
- Hash-based: Lamport (1979), Cramer-Shoup (2001)
- Latice based: NTRU (1998)
- codecrypt


Never ever give up!

review everything!

Deploy No

- verifiable builds
- gitian
- tahoe
- TLSv1.2
- nacl based crypto

Needs scrutiny

- viff
- OpenTransactions
- dust
- goldbug
- dissent
- steed
- TPM
- curvecp (clients?)
- pond
- cjdns

PBP

- difficult to fingerprint
- AE in symmetric
- ECC
- naive MPECDH

host security

- no private key on a default malware infected windows/mac host
- coreboot
- grsec/pax
- *F*DE (anakata?, firmware based backdoors)
- data minimization
- tails
- physical security
- external crypto devices

Cryptokey

- ARM Cortex M3
- 2.4GHz radio
- Small Display
- HWRNG
- 4 keys
- Battery
- USB
- MicroSD slot

other threats?

In a previous paper, we have shown that any Boolean formula can be encoded as a linear programming problem in the framework of Bayesian probability theory. When applied to NP-complete algorithms, this leads to the fundamental conclusion that $P = NP$. Now, we implement this concept in elementary arithmetic and especially in multiplication. This provides a polynomial time deterministic factoring algorithm, while no such algorithm is known to day. This result clearly appeals for a revaluation of the current cryptosystems. The Bayesian arithmetic environment can also be regarded as a toy model for quantum mechanics. - Michel Feldmann (2012), Polynomial time factoring algorithm using Bayesian arithmetic

Links

- Brands scheme in other words: http://www.orlingrabbe.com/stefbrdc.htm
- dust
- goldbug http://goldbug.sourceforge.net/
- dissent http://dedis.cs.yale.edu/2010/anon/
- gitian https://gitian.org/
- verifiable builds https://blog.torproject.org/blog/deterministic-builds-part-one-cyberwar-and-global-compr

Links. . .

- windows, nsa: http://www.heise.de/tp/artikel/5/5263/1.html
- lotus notes, nsa: http://www.heise.de/tp/artikel/2/2898/1.html
- ipsec: http://www.metzdowd.com/pipermail/cryptography/2013-September/017218.html
- rsa bsafe: http://blogs.wsj.com/digits/2013/09/19/rsa-dont-use-encryption-influenced-by-nsa/
- google mitm: http://www.techdirt.com/articles/20130910/10470024468/flying-pig-nsa-is-running-man-middle-attacks-imitating-shtml
- hardening: http://crunchbang.org/forums/viewtopic.php?id=24722

Credit/Legal

Stefan Marsiske, <s@ctrlc.hu>

pgp: FD52 DABD 5224 7F9C 63C6 3C12 FC97 D29F CA05 57EF
https://www.ctrlc.hu/~stef/stef.gpg

[1] https://creativecommons.org/licenses/by-sa/3.0/