NSA surprises, not ?

Jean-Philippe Aumasson (@veorq), Kudelski Security

This talk

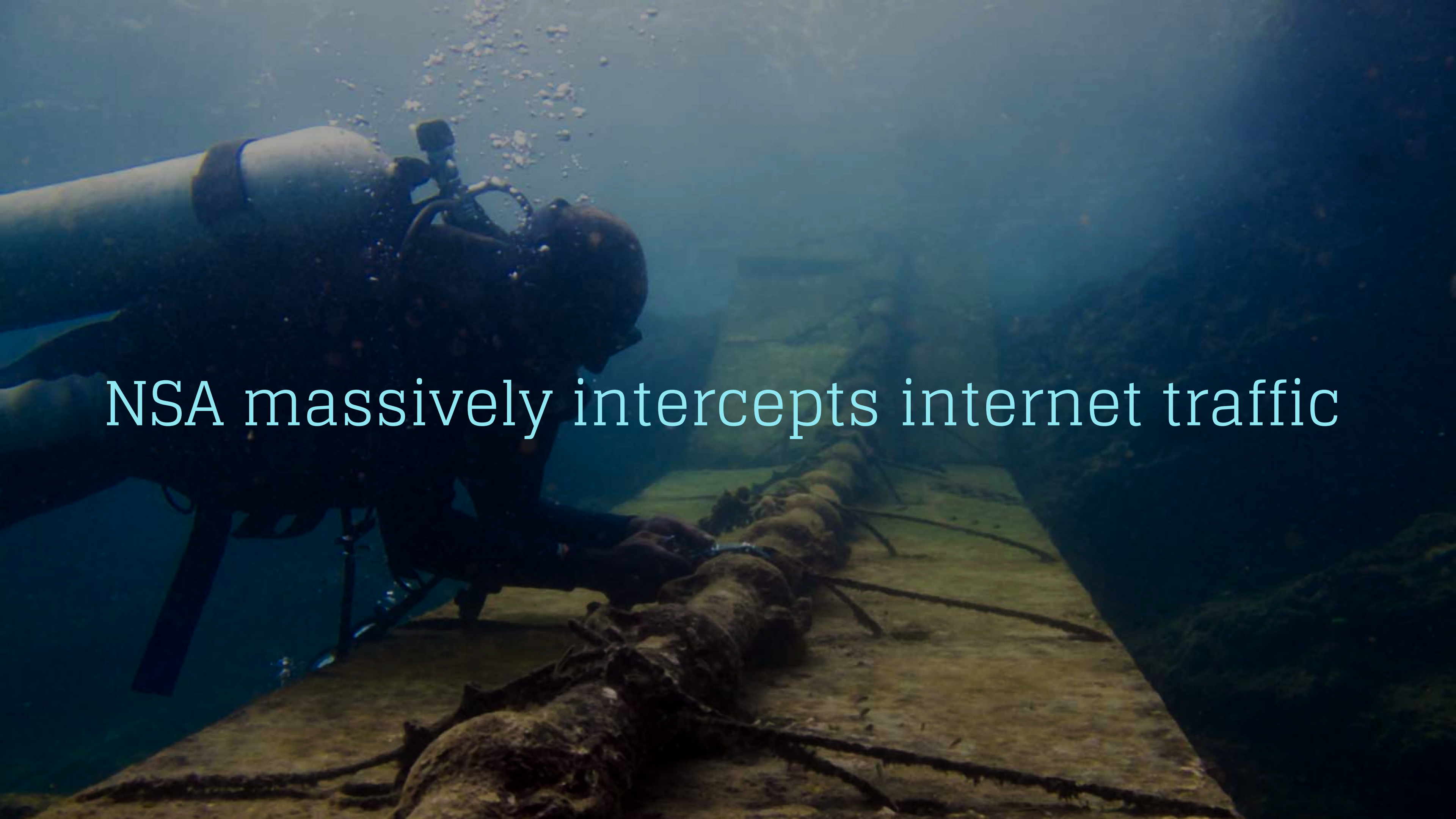
Facts and assumptions

Not political, moral, or legal issues

Doesn’t cover everything

part 1

Facts



NSA massively intercepts internet traffic

TEMPORA, XKeyScore, TURMOIL, etc.

Data and metadata collected, searchable

(U) Sensors: Passive Collection

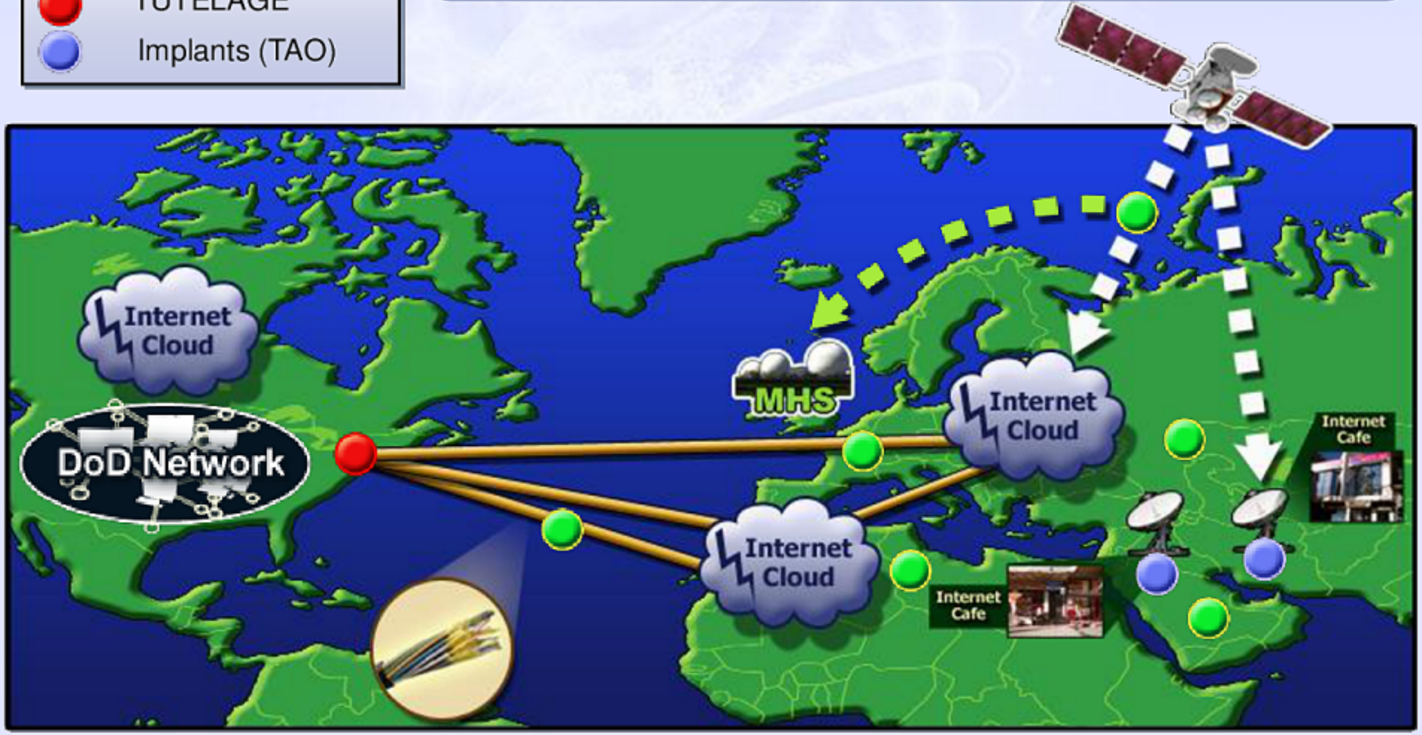
Accesses

🟢 TURMOIL

🔴 TUTELAGE

🔵 Implants (TAO)

TURMOIL (S//SI//REL) High-speed passive collection systems intercept foreign target satellite, microwave, and cable communications as they transit the globe.



NSA can inject and modify traffic

(U) There is More Than One Way to QUANTUM

TS//SI//REL

Name	Description	Inception Date	Status	Operational Success
CNE				
QUANTUMINSERT	• Man-on-the-Side technique • Briefly hi-jacks connections to a terrorist website • Re-directs the target to a TAO server (FOXACID) for implantation	2005	Operational	**Highly Successful** (In 2010, 300 TAO implants were deployed via QUANTUMINSERT to targets that were un-exploitable by any other means)
QUANTUMBOT	• Takes control of idle IRC bots • Finds computers belonging to botnets, and hijacks the command and control channel	Aug 2007	Operational	**Highly Successful** (over 140,000 bots co-opted)
QUANTUMBISCUIT	• Enhances QUANTUMINSERT's man-on-the-side technique of exploitation • Motivated by the need to QI targets that are behind large proxies, lack predictable source addresses, and have insufficient unique web activity.	Dec 2007	Operational	**Limited success at NSAW due to high latency on passive access** (GCHQ uses technique for 80% of CNE accesses)
QUANTUMDNS	• DNS injection/redirection based off of A Record queries. • Targets single hosts or caching name servers.	Dec 2008	Operational	**Successful** (High priority CCI target exploited)
QUANTUMHAND	Exploits the computer of a target who uses Facebook	Oct 2010	Operational	**Successful**
QUANTUMPHANTOM	Hijacks any IP on QUANTUMable passive coverage to use as covert infrastructure.	Oct 2010	Live Tested	**N/A**
CNA				
QUANTUMSKY	Denies access to a webpage through RST packet spoofing.	2004	Operational	**Successful**
QUANTUMCOPPER	File download/upload disruption and corruption.	Dec 2008	Live Tested	**N/A**

What if traffic is encrypted?

NSA may or may not decrypt it

(And metadata that is in clear still useful)

BULLRUN

- Covers the ability to defeat encryption used in specific network communications

- Includes multiple, extremely sensitive, sources and methods

Response to improving security

- For the past decade, NSA has lead an aggressive, multi-pronged effort to break widely used Internet encryption technologies
- Cryptanalytic capabilities are now coming on line
- Vast amounts of encrypted Internet data which have up till now been discarded are now exploitable

Key theft

Passive and **active** collection

(Exploit devices holding keys, etc.)

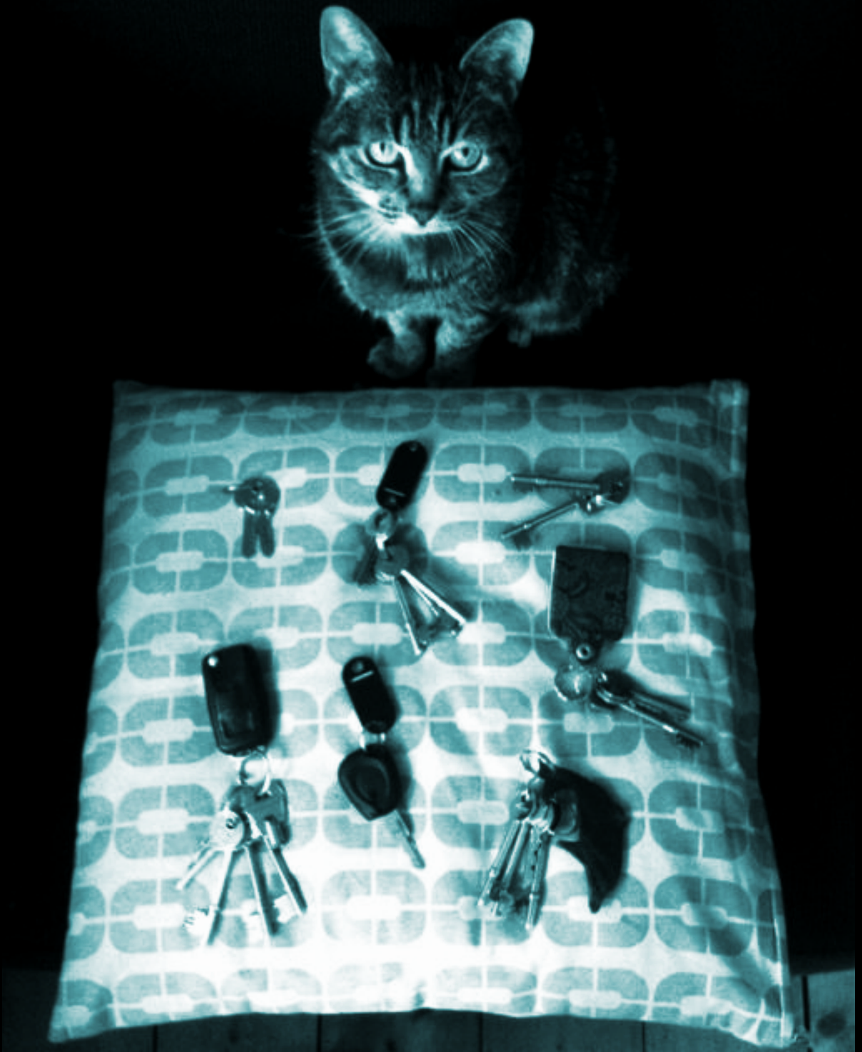
Static secrets for VPNs

(IPsec PSKs, SSH usernames/pwds, etc.)

Private keys of CA certs

(TLS interception)

SIM cards' subscriber keys



RSA Exploitation Steps

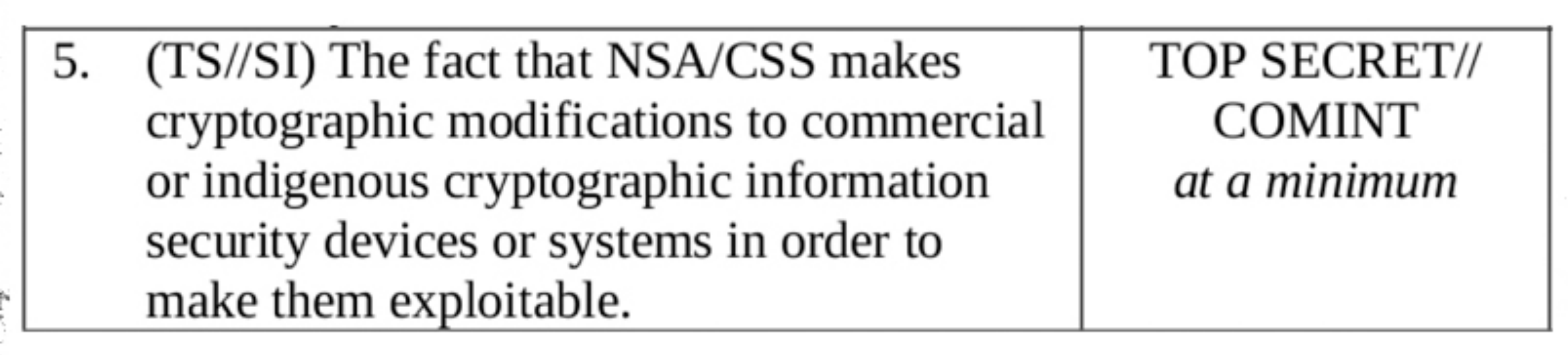
- Is it the key exchange RSA? (server hello)
  - If so, is the modulus match a known private key? (server certificate)
    - If so, is there 2-sided collect?
      - If so, do we have:
        - Client Hello
        - Server Hello
        - Client Key Exchange

DECRYPTION!

CNE access to core mobile networks

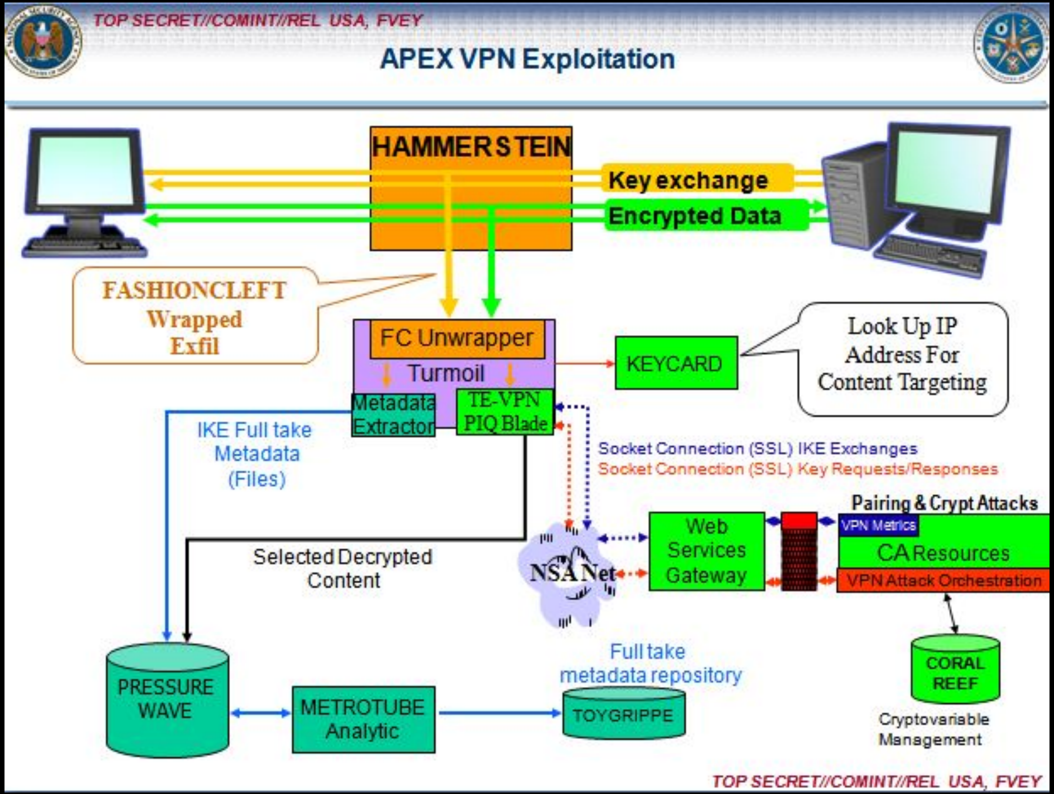
- CNE access to core mobile networks
  - Billing servers to suppress SMS billing
  - Authentication servers to obtain K's, Ki's and OTA keys
  - Sales staff machines for customer information and network engineers machines for network maps
  - GEMALTO – successfully implanted several machines and believe we have their entire network – TDSD are working the data

Sabotage of commercial systems



5. (TS//SI) The fact that NSA/CSS makes cryptographic modifications to commercial or indigenous cryptographic information security devices or systems in order to make them exploitable.	TOP SECRET// COMINT *at a minimum*

Exploitation, via “implants”



TOP SECRET//COMINT//REL USA, FVEY

APEX VPN Exploitation

HAMMERSTEIN
Key exchange
Encrypted Data
FASHIONCLEFT Wrapped Exfil
FC Unwrapper
Turmoil
Metadata Extractor
TE-VPN PIQ Blade
KEYCARD
Look Up IP Address For Content Targeting
IKE Full take Metadata (Files)
Socket Connection (SSL) IKE Exchanges
Socket Connection (SSL) Key Requests/Responses
Pairing & Crypt Attacks
VPN Metrics
CA Resources
VPN Attack Orchestration
Web Services Gateway
NSANet
Selected Decrypted Content
PRESSURE WAVE
METROTUBE Analytic
Full take metadata repository
TOYGRIPPE
CORAL REEF
Cryptovariable Management

TOP SECRET//COMINT//REL USA, FVEY

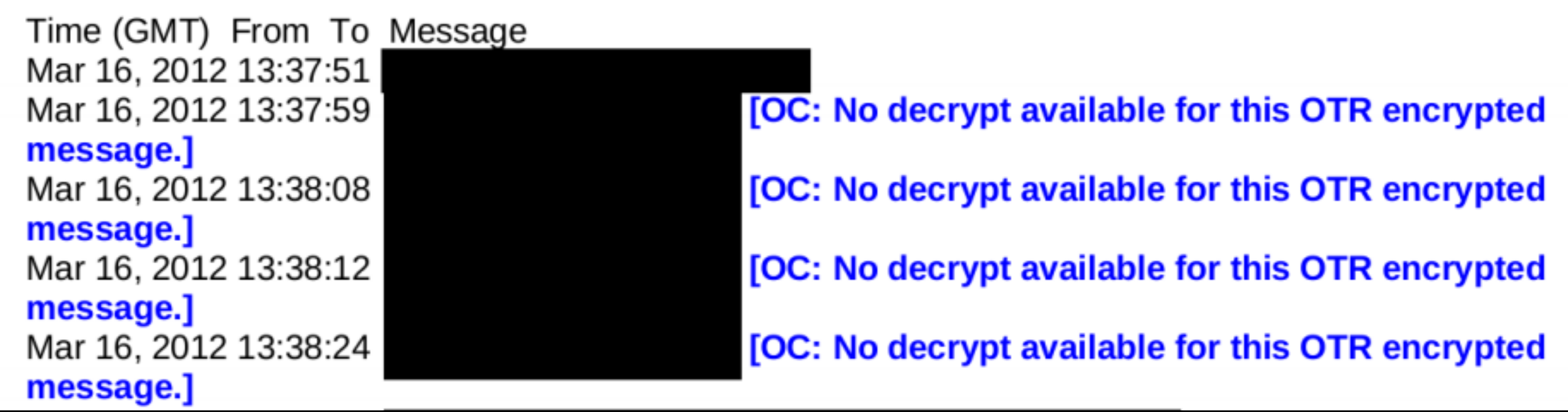
Cryptography circumvented

rather than “cracked”

Some protocols less prone to compromise

(No long-term secrets, forward secrecy end-to-end, etc.)

Off-the-record (OTR) chat



Time (GMT) From To Message

Mar 16, 2012 13:37:51 [redacted]

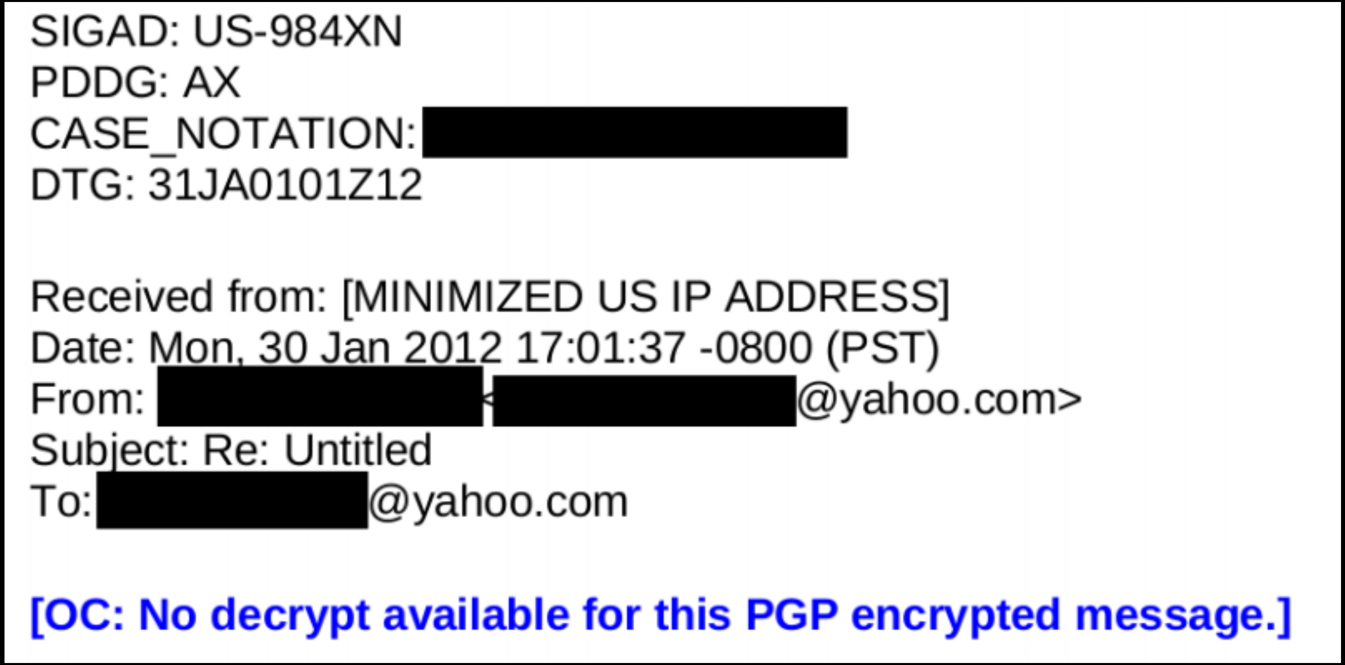
Mar 16, 2012 13:37:59 **[OC: No decrypt available for this OTR encrypted message.]**

Mar 16, 2012 13:38:08 **[OC: No decrypt available for this OTR encrypted message.]**

Mar 16, 2012 13:38:12 **[OC: No decrypt available for this OTR encrypted message.]**

Mar 16, 2012 13:38:24 **[OC: No decrypt available for this OTR encrypted message.]**

PGP email



SIGAD: US-984XN
PDDG: AX
CASE_NOTATION: [redacted]
DTG: 31JA0101Z12

Received from: [MINIMIZED US IP ADDRESS]
Date: Mon, 30 Jan 2012 17:01:37 -0800 (PST)
From: [redacted] <[redacted]@yahoo.com>
Subject: Re: Untitled
To: [redacted]@yahoo.com

[OC: No decrypt available for this PGP encrypted message.]

Proportionality

The higher value the target,
the more aggressive the methods

What about **cryptanalysis**?

“According to another top official also involved with the program, the NSA made an **enormous breakthrough** several years ago in its ability to cryptanalyze, or break, unfathomably complex encryption systems employed by not only governments around the world but also many average computer users in the US.”

James Bamford, March 2012
http://www.wired.com/2012/03/ff_nsadatacenter/all/1

part 2

Assumptions

Educated guesses

(Based on my and others’ knowledge and experience)

AES

Risk

Practical cryptanalytic attack

(TS//SI//REL) **TUNDRA** -- Electronic codebooks, such as the Advanced Encryption Standard, are both widely used and difficult to attack cryptanalytically. NSA has only a handful of in-house techniques. The TUNDRA project investigated a potentially new technique -- the Tau statistic -- to determine its usefulness in codebook analysis. This project was supported by [redacted] of R21.

[redacted]

(U) Summer Mathematics, R21, and the Director's Summer Program

(U) The Director's Summer Program (DSP) is the agency's premier summer program for mathematics undergraduates. Since its inception in 1990, the mission of the DSP has not been simply recruitment, (though a small but steady percentage of DSP participants do come back to work at NSA, often after obtaining an advanced degree), but rather an outreach effort aimed at attracting the best mathematics students from around the country, educating them about mathematics at NSA, and thus establishing ties with the future leaders of the outside mathematics community.

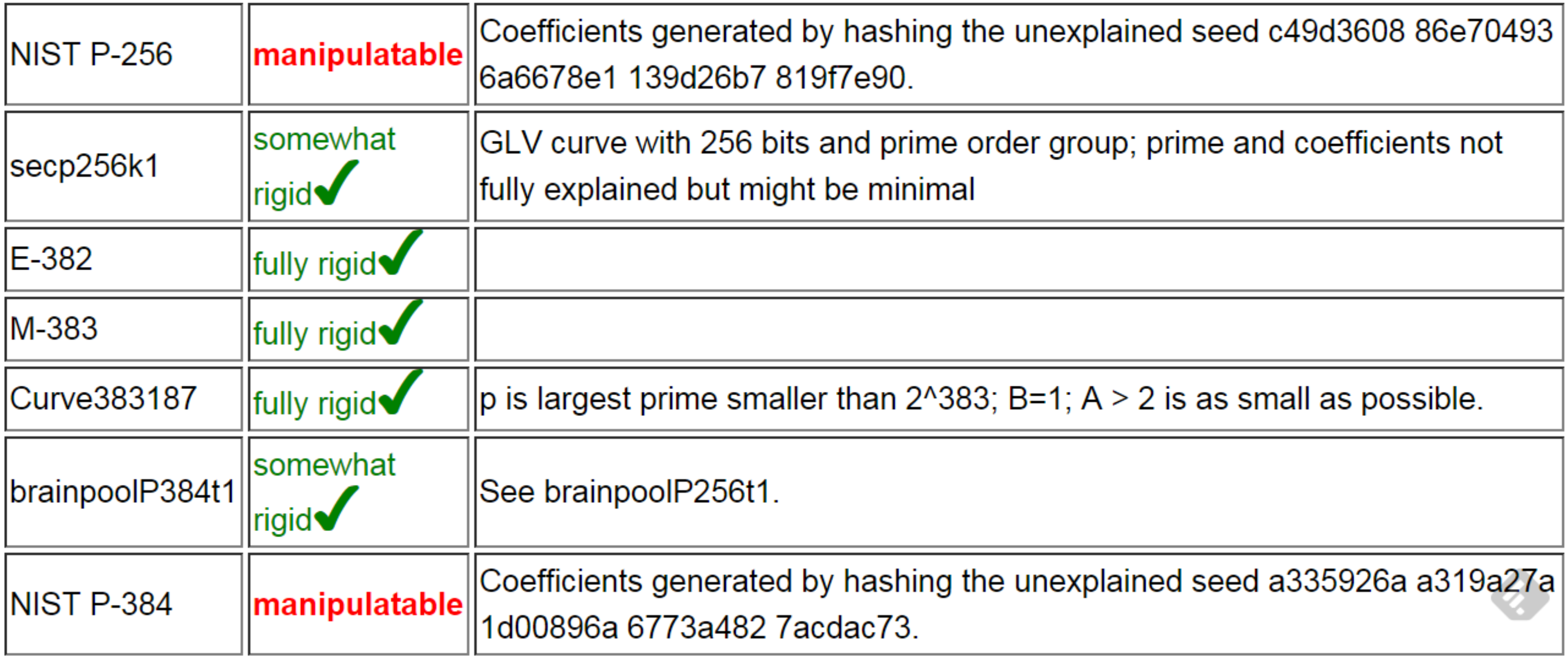
Assumption

The AES algorithm is and will remain safe

NIST elliptic curves

Risk

Weak/backdoored curves



NIST P-256	**manipulatable**	Coefficients generated by hashing the unexplained seed c49d3608 86e70493 6a6678e1 139d26b7 819f7e90.
secp256k1	somewhat rigid✓	GLV curve with 256 bits and prime order group; prime and coefficients not fully explained but might be minimal
E-382	fully rigid✓	
M-383	fully rigid✓	
Curve383187	fully rigid✓	p is largest prime smaller than 2^383; B=1; A > 2 is as small as possible.
brainpoolP384t1	somewhat rigid✓	See brainpoolP256t1.
NIST P-384	**manipulatable**	Coefficients generated by hashing the unexplained seed a335926a a319a27a 1d00896a 6773a482 7acdac73.

http://safecurves.cr.yp.to/rigid.html

Assumption

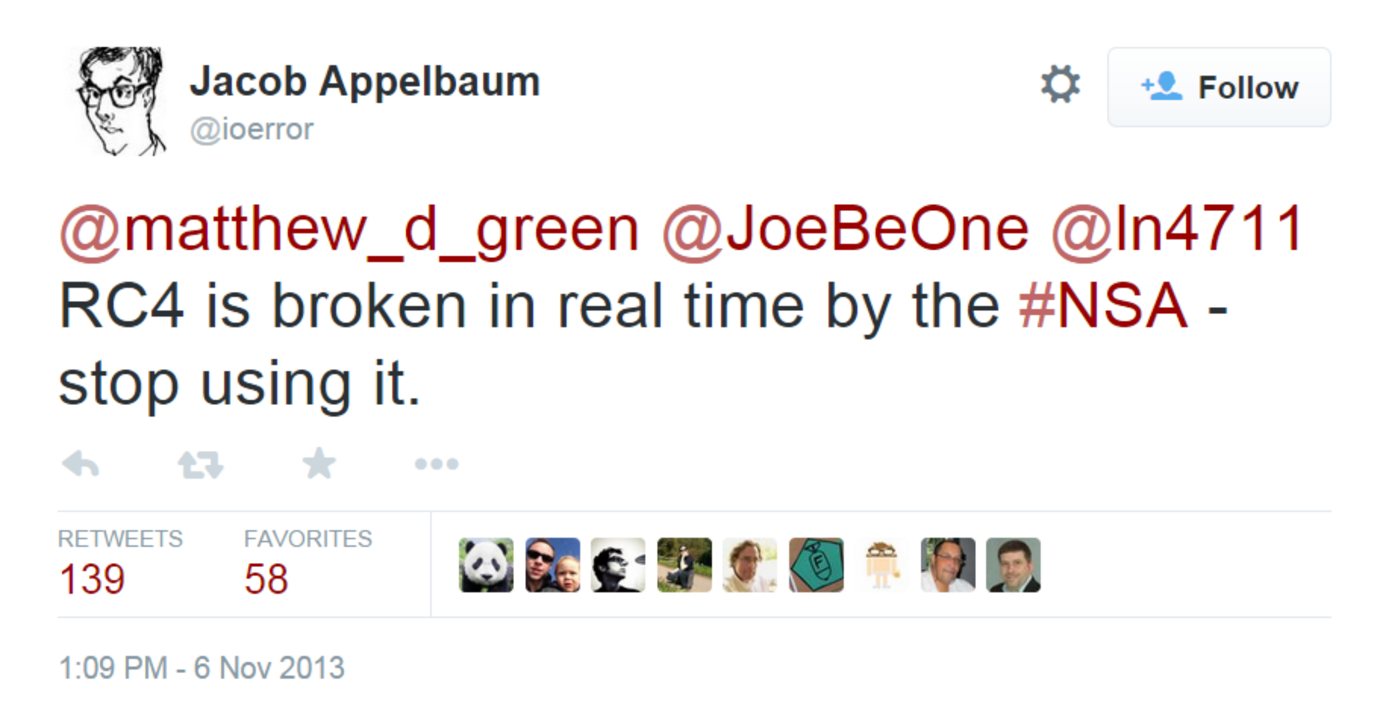
Fishy, but practical attack unlikely

Still, “rigid” curves better for confidence

RC4

Risk

Practical cryptanalytic attack



Jacob Appelbaum
@ioerror

@matthew_d_green @JoeBeOne @In4711 RC4 is broken in real time by the #NSA - stop using it.

RETWEETS 139 FAVORITES 58

1:09 PM - 6 Nov 2013

Assumption

Insecure

RSA

Risk

Factoring breakthrough

Picture credit: Rick Bowmer/AP

How to use
the new 65-megawatt
Bluffdale supercomputer:
a gentle introduction
to cryptanalysis

D. J. Bernstein
University of Illinois at Chicago &
Technische Universiteit Eindhoven

Disclaimers

1. I don't work for NSA.
2. NSA hasn't told me anything.
3. This is not a leak.
4. I'm *assuming* that NSA is not stupid.
5. Also *assuming* use of traditional transistors+wires, probably with some optics; plus long-term storage. Quantum computing would require different analysis.

Obvious solution for NSA:
some ASICs, plus heterogeneous
mix of **application-tuned**
integrated circuits (ATICs).

Take a general-purpose CPU.
Add exactly the big insn
XYZZY needed by application,
plus some vectorization.
Think ahead, add agility:
XYZZ? XZZY? XYQZZY?
Still similar cost to ASIC.

New CPU for each application.
Merge similar applications
if not much cost in area.

1-slide Bluffdale user guide

Critical for algorithm designer
and implementor:

Massive parallelism.

Grid communication.

Multiple instruction sets
with very useful instructions.

Some vectorization.

Occasional faults.

Need to understand cryptanalysis:
ECM, sparse linear algebra,
differentials, FFTs, much more.

Assumption

No major algorithmic advance

(In particular, no polytime algorithm)

But 1024-bit factoring may be doable

(For high-value targets, when other methods failed)

Quantum computer

Risk

Scalable system against factoring, discrete log, etc.

PUBLICATION DATE: (U) 21 September 2011

OFFICE OF ORIGIN: (U) The Laboratory for Physical Sciences/R3

POC: (U//FOUO) [redacted]

ORIGINAL CLASSIFICATION AUTHORITY: (U) [redacted], [redacted] [redacted], Community Integration, Policy and Records

(U//FOUO) This document establishes information security guidelines on NSA/CSS-sponsored research in the field of quantum computing (QC). The objectives defining the scope of this research activity are:

1) (S//REL) To assess if it is to NSA's benefit to continue research into whether practical-scale QC can be developed within a reasonable timeframe, to identify its most promising physical embodiment(s), and to formulate a credible scenario for its large-scale development;

2) (U//FOUO) To gain an understanding of the computational cryptanalytic capabilities of quantum computers; and

3) (U//FOUO) To identify practical cryptographic methods that are not susceptible to quantum computational attack.

(S//REL) These guidelines *do not* cover the possibility of large-scale cryptologic QC development programs at NSA, but only the research and planning preliminary to, and in possible support of, such programs.

(S//SI//REL) Much of the research in quantum computing is still very basic and is most effectively pursued in NSA-funded open research programs. These programs play a critical role as the major source of new ideas and for training future researchers in the field. However, NSA is pursuing more than just basic, unclassified research. NSA is also attempting to preserve the SIGINT potential of quantum computing (i.e., the cryptanalytic applications of QC) while simultaneously attempting to protect the information security of both the Government and private sectors against hostile QC attacks (i.e., the cryptographic, mission assurance applications of QC of interest to the Information Assurance community). These goals must be pursued at the classified level.

Assumption

As far from a working system as public research

Tor

Risks

Deanonymization capabilities

Tor Stinks… (U)

- We will never be able to de-anonymize all Tor users all the time.
- With manual analysis we can de-anonymize a **very small fraction** of Tor users, however, **no** success de-anonymizing a user in response to a TOPI request/on demand.

Assumption

No mass deanonymization,
but progress since pre-2010 documents

And always, deanonymization from OPSEC failures part 3

Conclusions

NSA is to SIGINT what **Mossad** is to HUMINT

(Aggressive, by-all-means-necessary approach)

Interception, sabotage, exploitation

Surprising breadth and depth

Cryptanalysis

No surprise, so far

Why attacking the strongest link?

Thank you

NSA documents archive: http://cryptome.org/2013/11/snowden-tally.htm

Title page visuals: https://citizenfourfilm.com/

Contact: jeanphilippe.aumasson@gmail.com | http://aumasson.jp | @veorq