Crypto Wars 2.0

Abertay Hackers
Michael Jack

mikey$ whoami

- Michael Jack
- 2nd Year Ethical Hacking BSc @ Abertay
- Member Abertay Ethical Hacking Society
- I <3 Cryptography

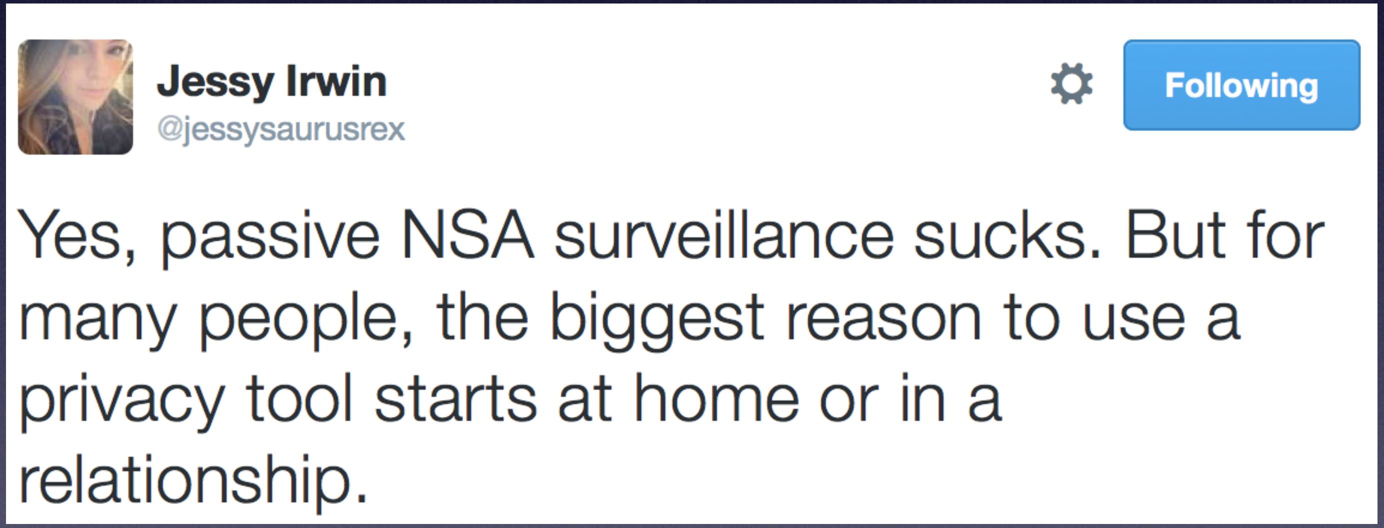
- @MikeyJck
- mikeyjck.io

What’s all this then?

- Quick history of modern cryptography
- background on first Crypto Wars circa 1990s
- second crypto wars circa 2012
- wrap up
- 🍺

before we begin

"At ever single level we as a community have forgotten that privacy as well as security need to be a goal" - Brendan O'Connor Defcon 21



Jessy Irwin
@jessysaurusrex

Yes, passive NSA surveillance sucks. But for many people, the biggest reason to use a privacy tool starts at home or in a relationship.

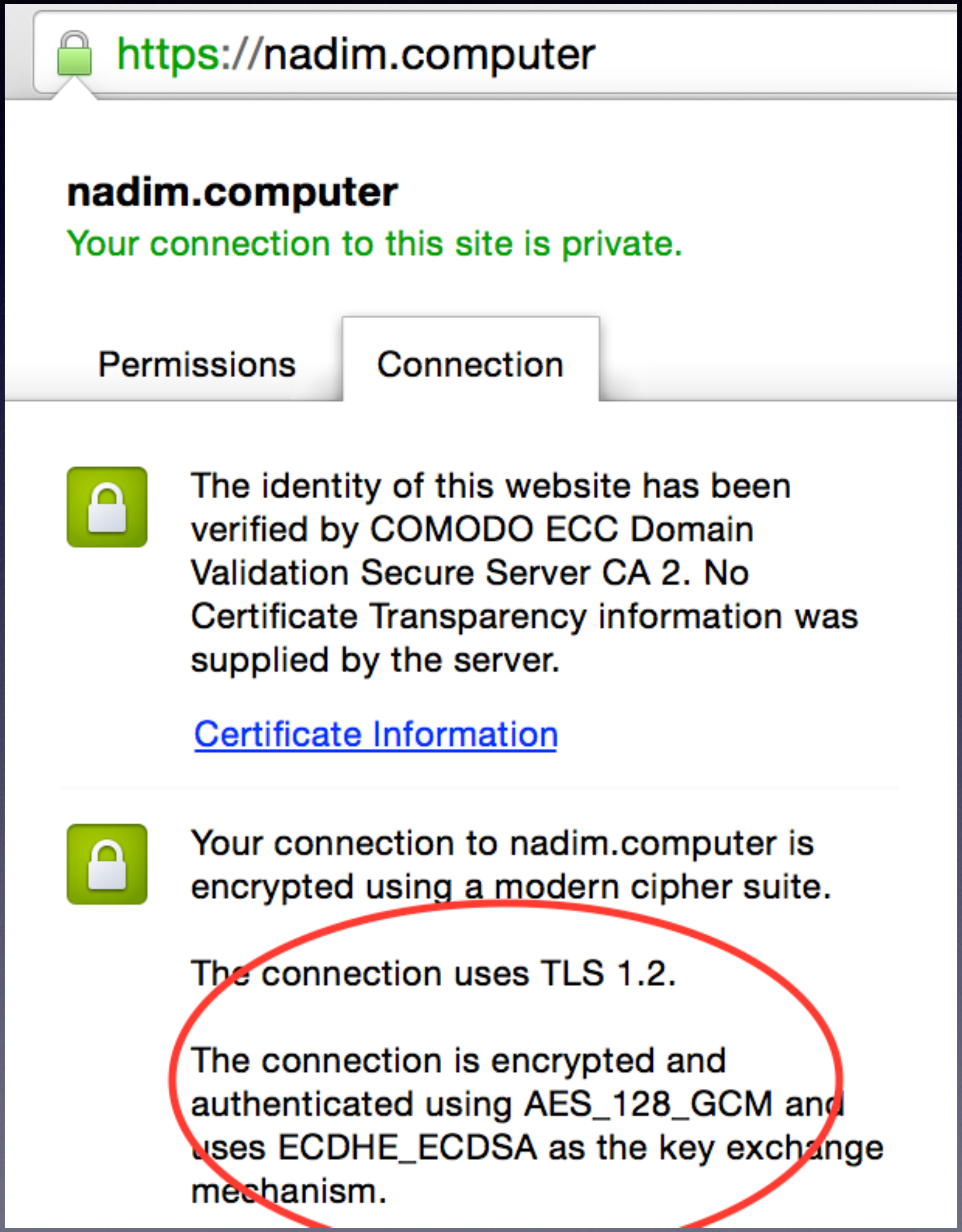
Modern Cryptography

2015

- Data at Rest = AES or PGP
- Data in Motion = TLS1.2 or IPSEC
- Data in air = WPA2 or SNOW 3G(?)

The Internet

- Elliptic Curve
- Diffie-Hellman
- EC Digital Signature Algorithm
- 128-bit AES GCM mode
- Protocol: TLS 1.2
  - *discrete log modulo prime (DSA)*



https://nadim.computer

nadim.computer

Your connection to this site is private.

The identity of this website has been verified by COMODO ECC Domain Validation Secure Server CA 2. No Certificate Transparency information was supplied by the server.

Certificate Information

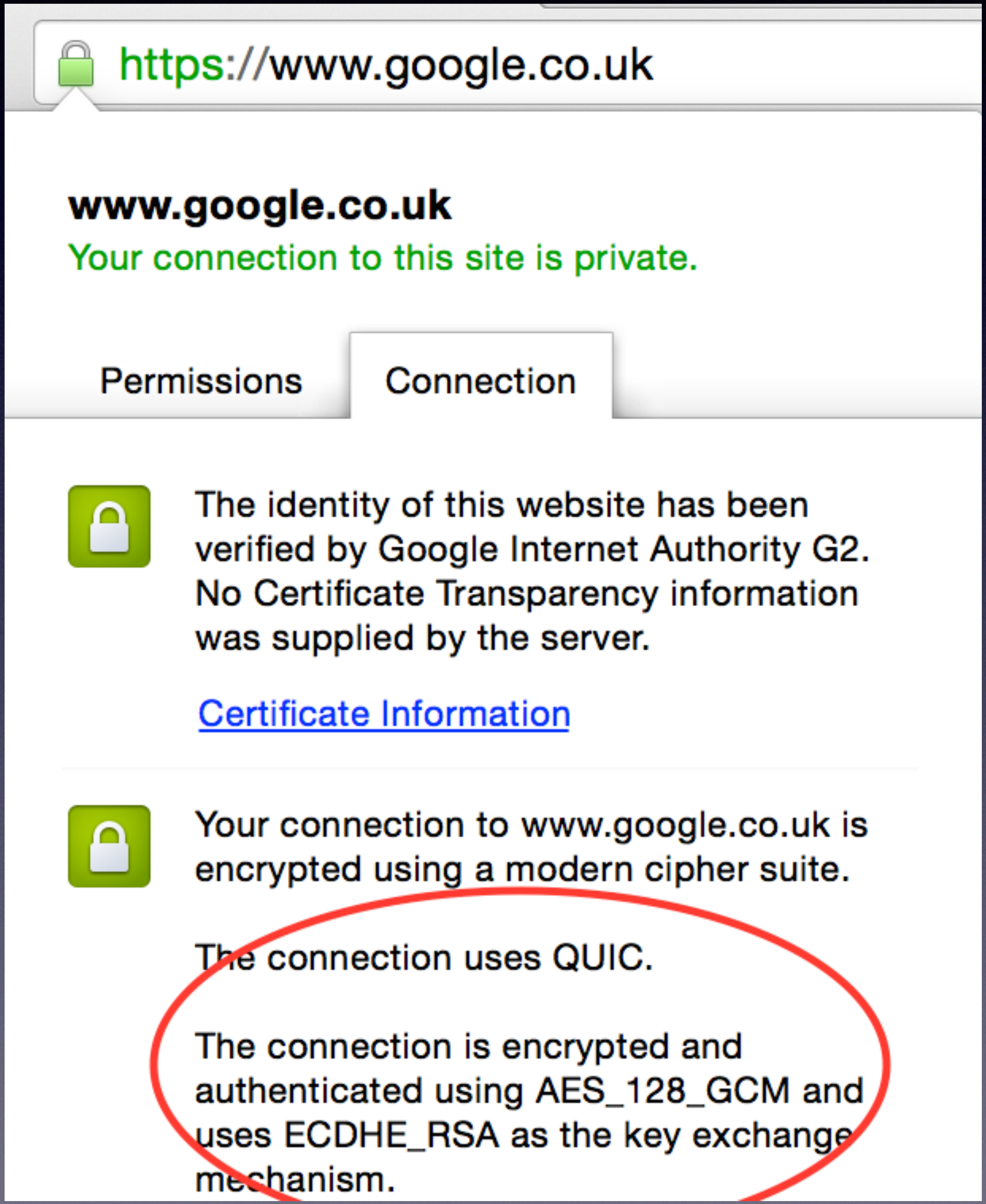
Your connection to nadim.computer is encrypted using a modern cipher suite.

The connection uses TLS 1.2.

The connection is encrypted and authenticated using AES_128_GCM and uses ECDHE_ECDSA as the key exchange mechanism.

The (Google's) Internet

- Elliptic Curve
- Diffie-Hellman
- RSA
- 128-bit AES GCM mode
- Protocol: QUIC
  - *discrete log in elliptic curve groups (ECDH)*
  - *factoring integers into primes (RSA)*



https://www.google.co.uk

www.google.co.uk

Your connection to this site is private.

Permissions | Connection

The identity of this website has been verified by Google Internet Authority G2. No Certificate Transparency information was supplied by the server.

Certificate Information

Your connection to www.google.co.uk is encrypted using a modern cipher suite.

The connection uses QUIC.

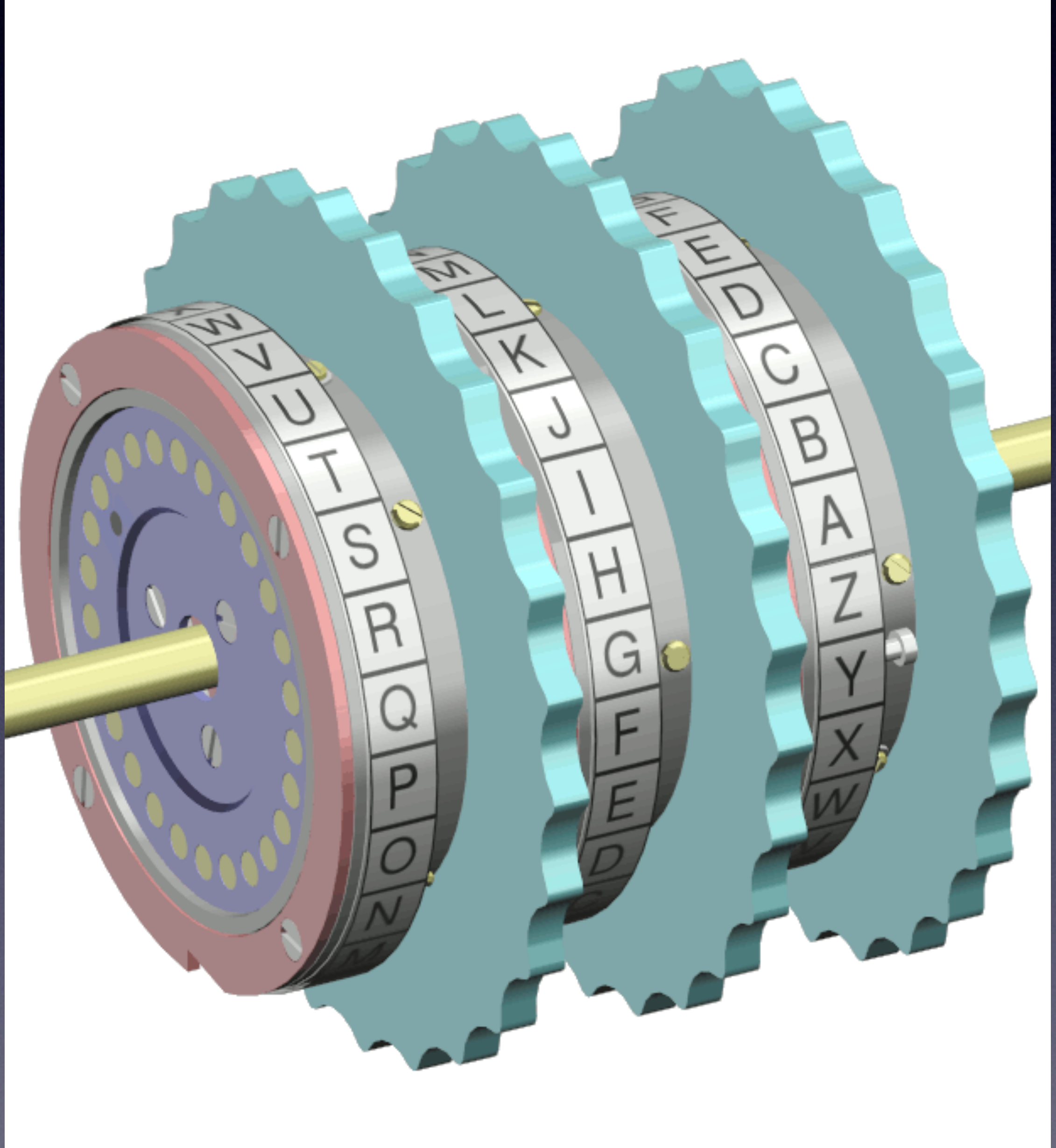
The connection is encrypted and authenticated using AES_128_GCM and uses ECDHE_RSA as the key exchange mechanism.

What is Modern Crypto?

- Colossus - Newman, Flowers et al @ Bletchley
    - post World War II
- more accurately 1970s >
- NSA, GCHQ, IBM & Bell Labs

World War II

- Enigma (electromechanical)
- Broken by Marian Rejewski et al
- Continued decryption by Turning, Welchman et al @ Bletchley Park



Timeline 0x01

- 1971 - IBM Lucifer Block Cipher (Watson Lab) Feistel
- 1973 - NBS asks for Data Encryption Standard (DES) designs
- 1973-4 - IBM develop & submit DES candidate
- 1974 - IBM discovers Differential Cryptanalysis, NSA gag order
- 1976 - Diffie & Hellman publish “New Directions in Cryptography”
- 1976 - After alterations by NSA IBMs design chosen as DES
- 1977 - “Method for Obtaining Digital Signatures and Public-Key Cryptosystems" by Rivest, Shamir & Adleman (RSA) @ MIT

Timeline 0x02

- 1971 - IBM Lucifer Block Cipher (Watson Lab)
- 1973 - NBS asks for Data Encryption Standard (DES) designs
- 1973-4 - IBM develop & submit DES candidate
- 1973 - RSA invented by GCHQ (Cocks)
- 1974 - DH invented by GCHQ (Williamson)
- 1974 - IBM discovers Differential Cryptanalysis, NSA gag order
- 1976 - Diffie & Hellman publish “New Directions in Cryptography”
- 1976 - After alterations by NSA IBMs design chosen as DES
- 1977 - “Method for Obtaining Digital Signatures and Public-Key Cryptosystems" by Rivest, Shamir & Adleman (RSA) @ MIT

Timeline 0x03

- 1984 - RC4 Stream Cipher RSA Labs (Rivest)
- 1991 - Pretty Good Privacy (PGP) Phil Zimmerman
- 1994 - Secure Sockets Layer (SSL) conceived @ Netscape
- 1999 - SSL Standardised by IETF > Transport Layer Security (TLS)
- 1999 - NIST wants DES successor > public competition for Advanced Encryption Standard (AES)
- 1999 - Wired Equivalent Privacy (WEP) RC4

Timeline 0x04

- 2001 - NIST approves Rijndael for use as AES (FIPS 197)
- 2001 FIPS 180-4 released as SHA2
- 2004 - Wi-fi Protected Access 2 (WPA2)
- 2008 - TLS 1.2 RFC 5246
- 2015 - SHA3 (Keccak) standardised as FIPS 202
- 2015 - SHA1 Freestart collision

Crypto Wars 2.0

Politics & Policy

‘Going Dark’

- As early as 2011 FBI talking about the issue to congressional committees
- iOS 8 (2014) Full Disk Encryption by default
- Android 6 (2015) stock & OEM FDE by default

Crypto VIPs

Late 2014 LE/ politicians call for crypto backdoors

- FBI Director - James Comey
- GCHQ Director - Robert Hannigan
- MET Commissioner - Bernard Hogan-Howe
- UK Prime Minister - David Cameron
- UK Home Secretary - Theresa May

Correcting Misconceptions

James Comey Oct 2014

"misconception that building a lawful intercept solution… requires a so-called "back door," **one that foreign adversaries and hackers may try to exploit.**

But that isn't true. We aren't seeking a back-door **approach**. We want to use the front door, with clarity and transparency, and with clear guidance provided by law."

“One is communications data, that is not the content of a phone call. It is **just** who made which call to which person and when… And what matters, in simple terms is that we can access this data [on all platforms]… I have a very simple principle to apply here… in our country do we want to allow a means of communication that **in extremis we can’t read with a signed warrant…**”

– David Cameron January 2015

Bullrun & Edgehill

TOP SECRET/ STRAP1

nsa$ whoami

National Security Agency

- 2013 Budget: $10.8B
  - $2.5B on data collection
  - $1.6B on processing/ exploitation
- Upwards of 40k employees
- Created by Truman in secret 1952
- FISA/ National Security Letters/CALEA

gchq$ whoami

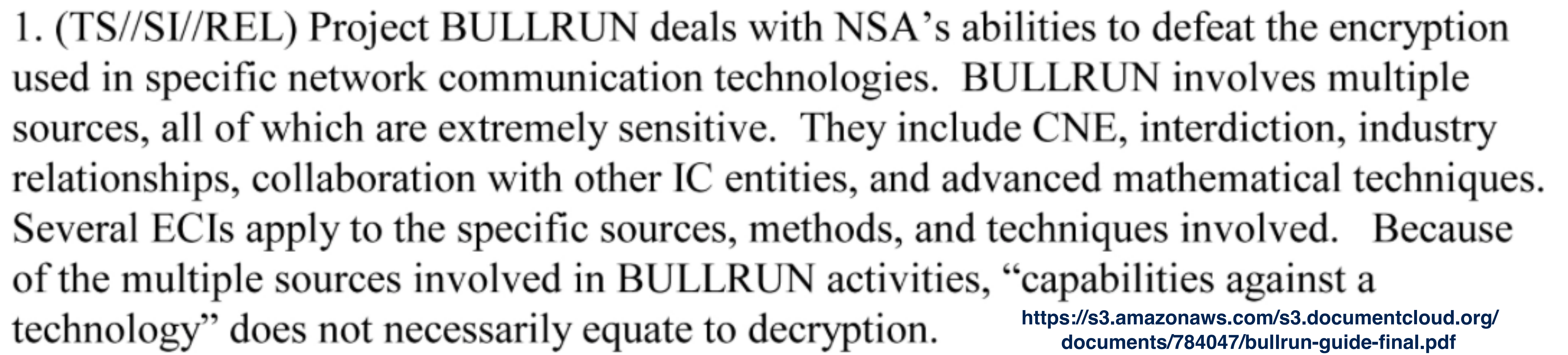
Government Communications HQ

- Originally founded 1919 as GC&CS
- Unique access to backbone infrastructure
- Upwards of 6k employees
- RIPA

Cryptanalysis is good

BULLRUN

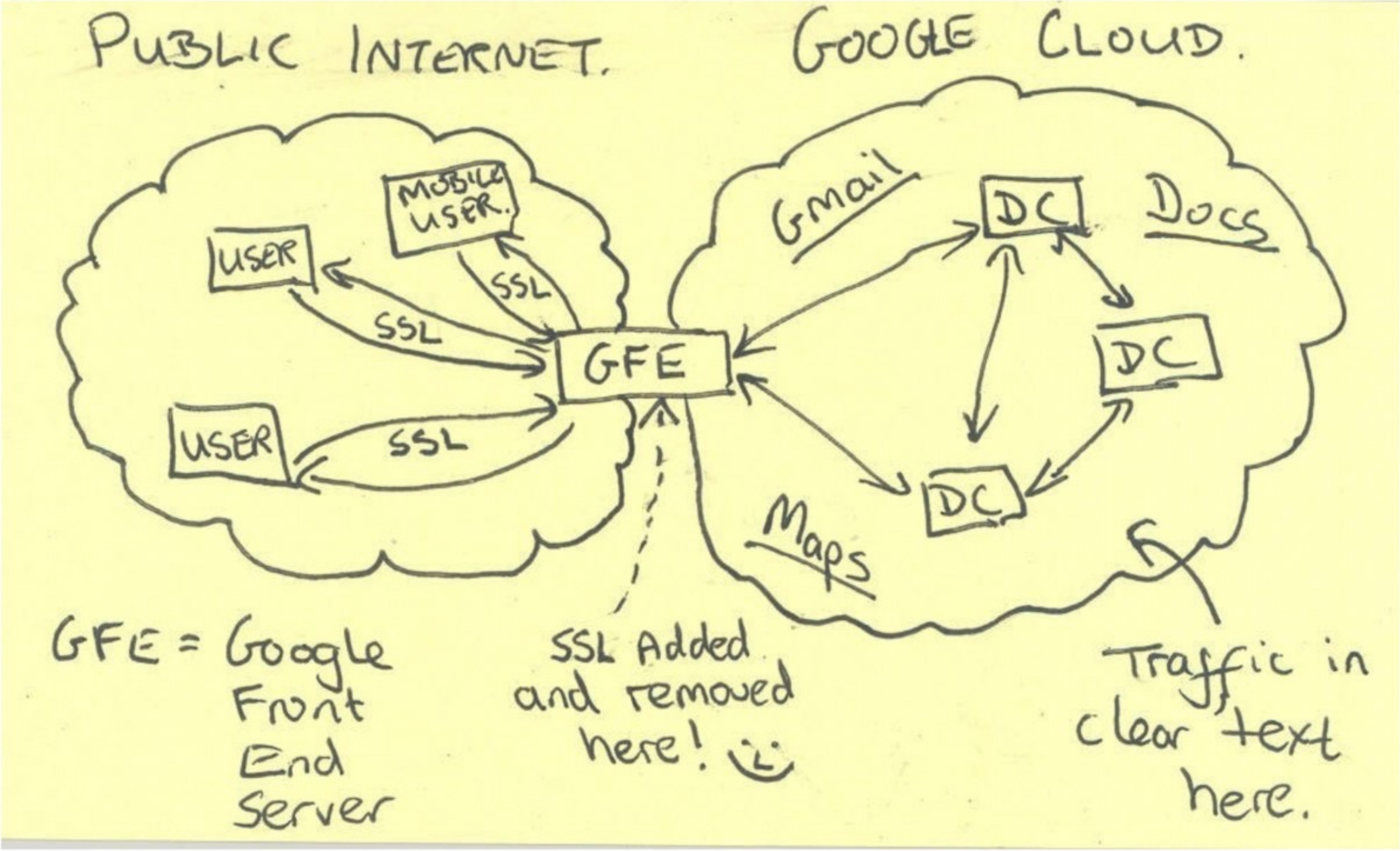
- Ability to defeat encryption
- BULLRUN sources "extremely sensitive"
- TLS/ SSH/ OTR/ VPN/ VoIP/ etc



1. (TS//SI//REL) Project BULLRUN deals with NSA's abilities to defeat the encryption used in specific network communication technologies. BULLRUN involves multiple sources, all of which are extremely sensitive. They include CNE, interdiction, industry relationships, collaboration with other IC entities, and advanced mathematical techniques. Several ECIs apply to the specific sources, methods, and techniques involved. Because of the multiple sources involved in BULLRUN activities, "capabilities against a technology" does not necessarily equate to decryption.

https://s3.amazonaws.com/s3.documentcloud.org/documents/784047/bullrun-guide-final.pdf

Current Efforts - Google


PUBLIC INTERNET.
GOOGLE CLOUD.
MOBILE USER.
USER
SSL
SSL
USER
SSL
SSL
GFE
Gmail
DC
Docs
DC
DC
DC
Maps
GFE = Google Front End Server
SSL Added and removed here! ☺
Traffic in clear text here.

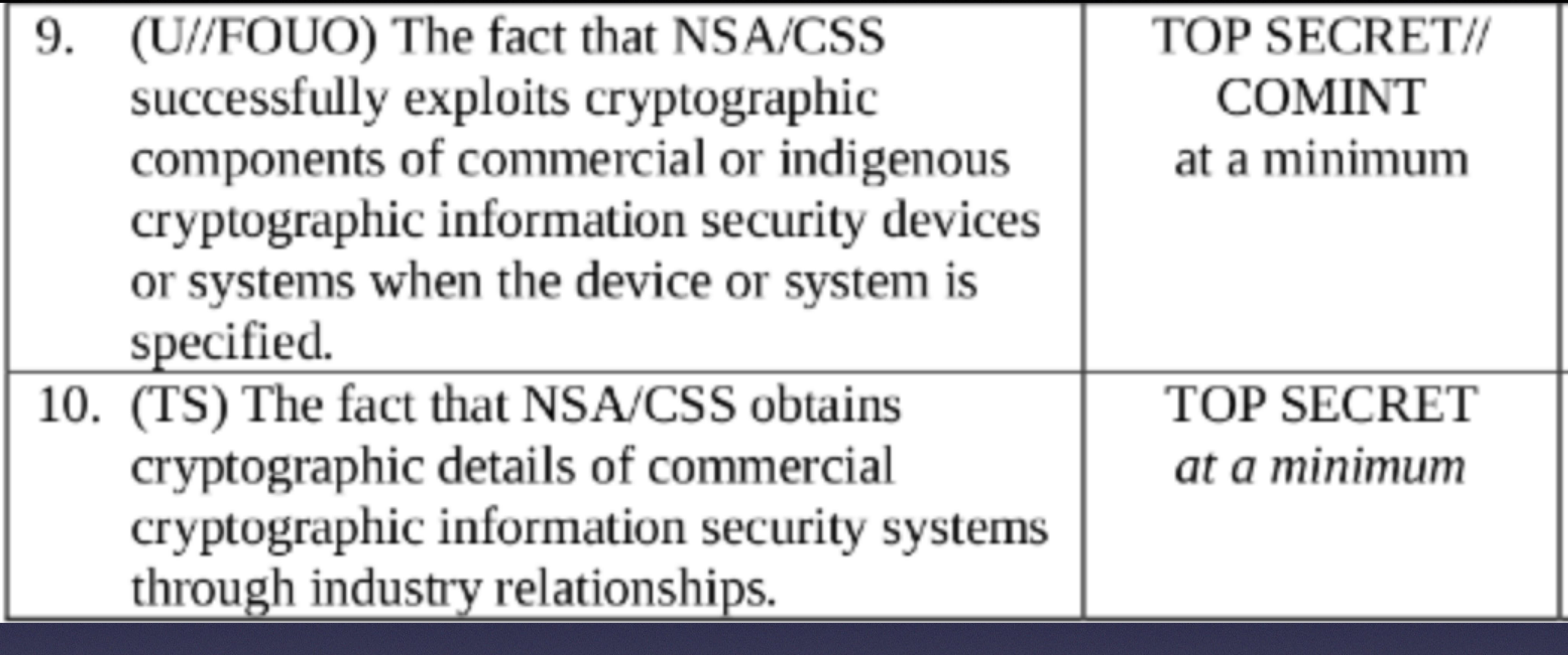
MUSCULAR

Response to improving security

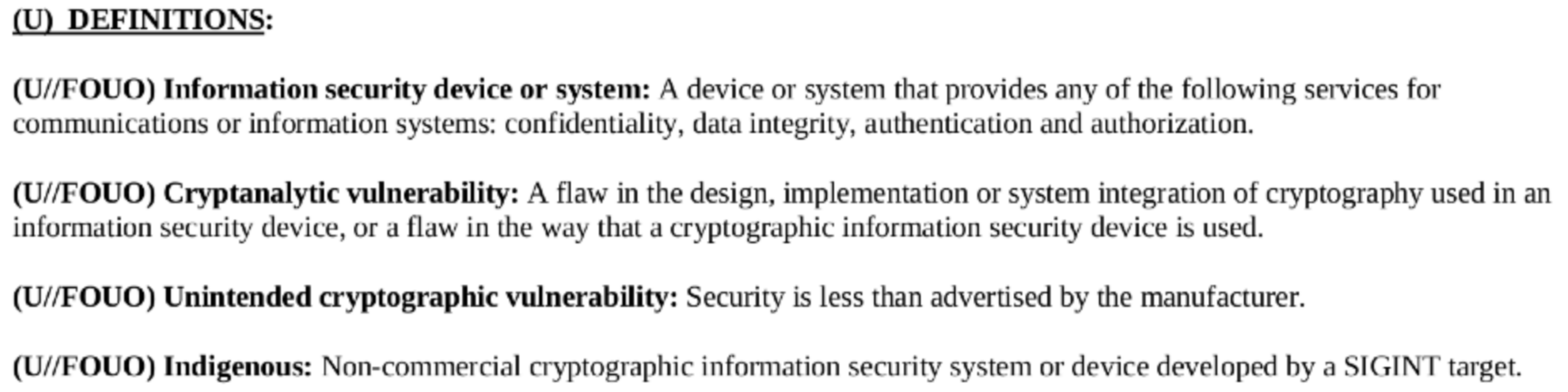
- For the past decade, NSA has lead an aggressive, multi-pronged effort to break widely used Internet encryption technologies
- Cryptanalytic capabilities are now coming on line
- Vast amounts of encrypted Internet data which have up till now been discarded are now exploitable
- Major new processing systems, SIGDEV efforts and tasking must be put in place to capitalize on this opportunity

Protecting the Info – Secure COI

- Secure Community of Interest (COI) – protects “fact of” as well as volume and scope of the capability
- BULLRUN indoctrination required for access to COI
- BULLRUN-related material, data – decrypted content and decrypted metadata, and details must be protected within the COI



9.	(U//FOUO) The fact that NSA/CSS successfully exploits cryptographic components of commercial or indigenous cryptographic information security devices or systems when the device or system is specified.	TOP SECRET// COMINT at a minimum
10.	(TS) The fact that NSA/CSS obtains cryptographic details of commercial cryptographic information security systems through industry relationships.	TOP SECRET *at a minimum*



(U) DEFINITIONS:

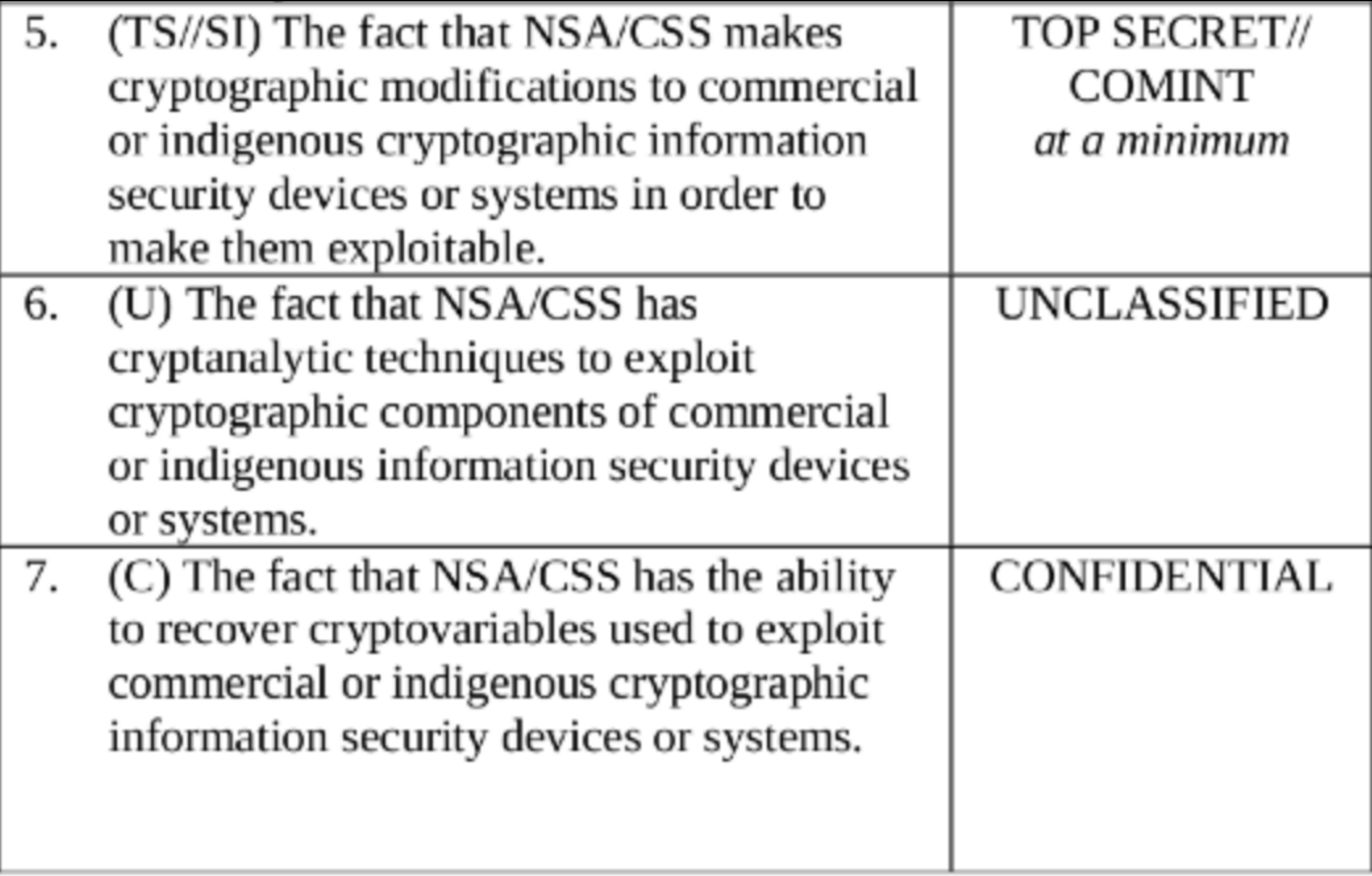
(U//FOUO) **Information security device or system:** A device or system that provides any of the following services for communications or information systems: confidentiality, data integrity, authentication and authorization.

(U//FOUO) **Cryptanalytic vulnerability:** A flaw in the design, implementation or system integration of cryptography used in an information security device, or a flaw in the way that a cryptographic information security device is used.

(U//FOUO) **Unintended cryptographic vulnerability:** Security is less than advertised by the manufacturer.

(U//FOUO) **Indigenous:** Non-commercial cryptographic information security system or device developed by a SIGINT target.

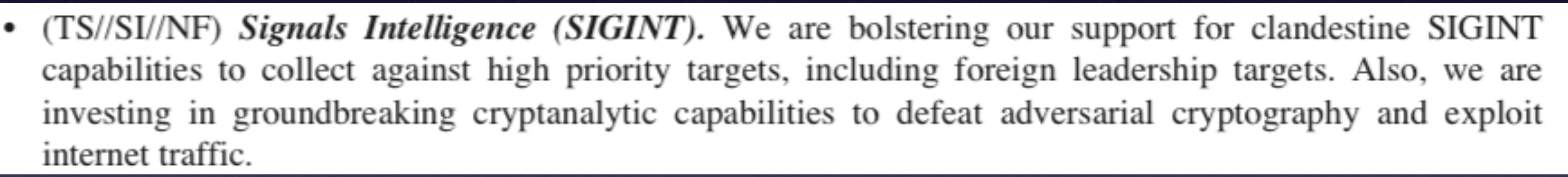
www.spiegel.de/media/media-35546.pdf



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*
6. (U) The fact that NSA/CSS has cryptanalytic techniques to exploit cryptographic components of commercial or indigenous information security devices or systems.	UNCLASSIFIED
7. (C) The fact that NSA/CSS has the ability to recover cryptovariables used to exploit commercial or indigenous cryptographic information security devices or systems.	CONFIDENTIAL

Circa September 2005

www.spiegel.de/media/media-35546.pdf



- (TS//SI//NF) ***Signals Intelligence (SIGINT).*** We are bolstering our support for clandestine SIGINT capabilities to collect against high priority targets, including foreign leadership targets. Also, we are investing in groundbreaking cryptanalytic capabilities to defeat adversarial cryptography and exploit internet traffic.

National Intelligence Budget 2013
DNI Statement

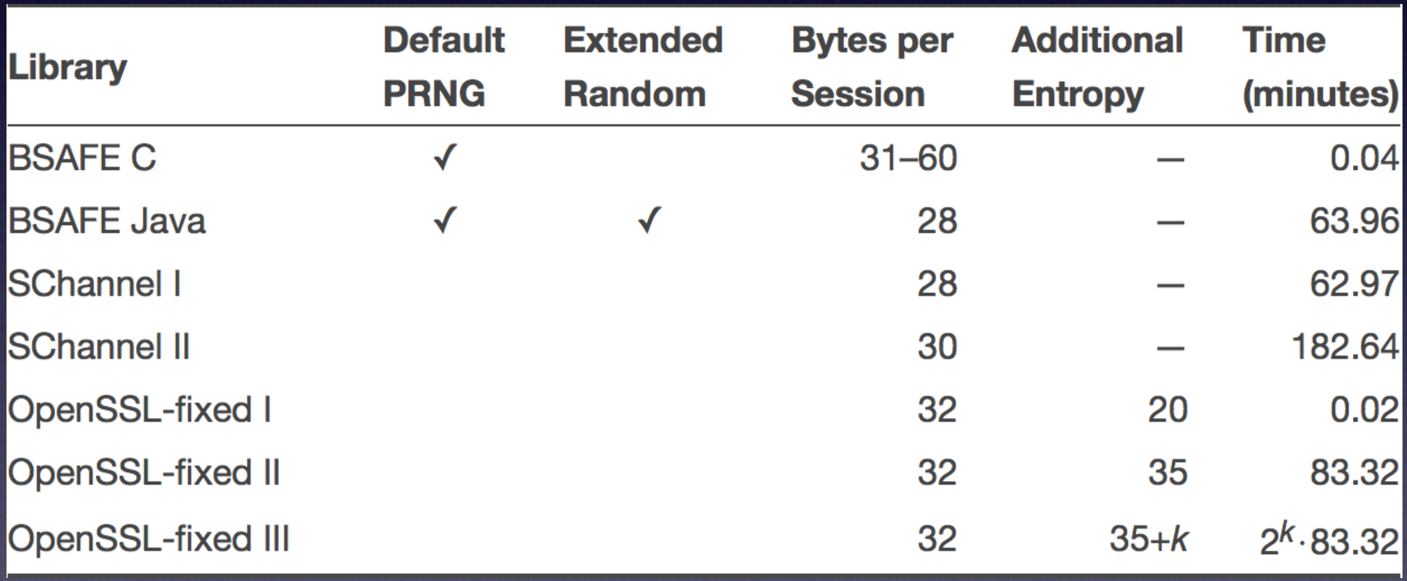
The Curious Case of the Dual_EC_DRBG

here be backdoors

- RSA accepted $10M from NSA to use Dual EC DRBG as default in BSAFE library (2004/5)
- RSA “relied on guidance from NIST”
- RSA claim they didn’t know it was weakened or contained a backdoor
- Dual_EC_DRBG withdrawn after NIST issues new guidlines Sept 2013

math

- Constants that define the EC
- should be random
- NIST doesn't say how or where the constants come from
- If these constants were picked specially there is a ‘skeleton key’
- after recovery of 32bytes of output attacker can predict DRBG output

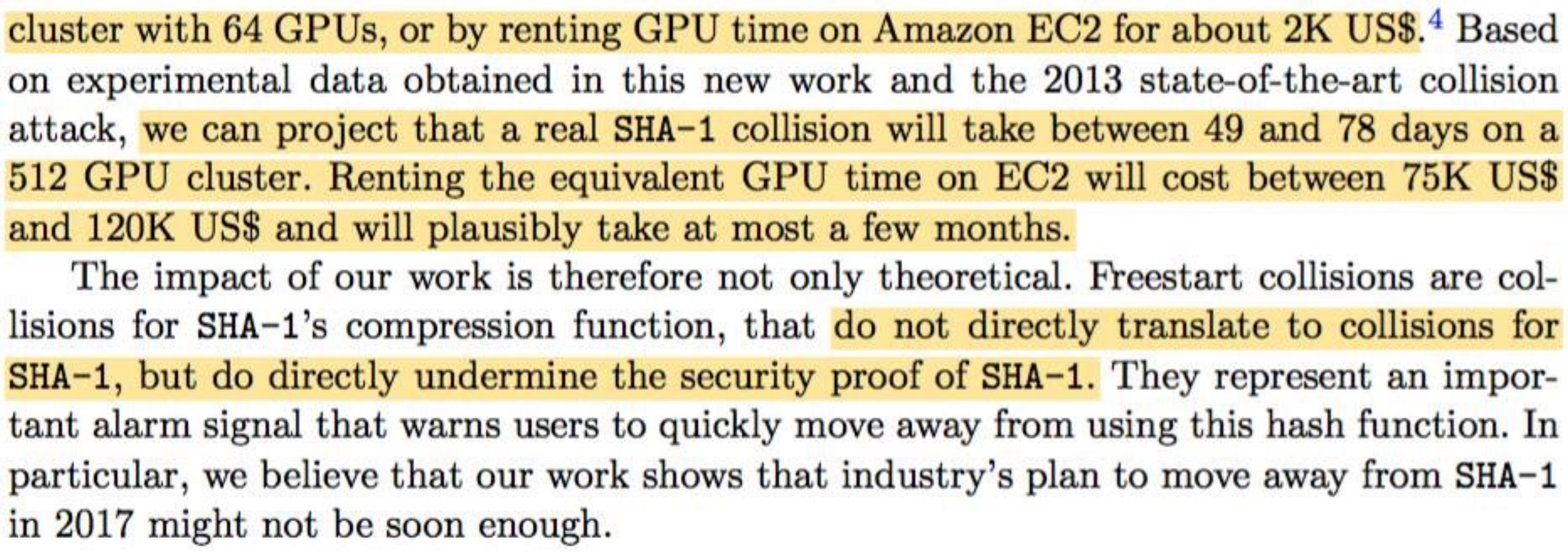


Library	Default PRNG	Extended Random	Bytes per Session	Additional Entropy	Time (minutes)
BSAFE C	✓		31–60	—	0.04
BSAFE Java	✓	✓	28	—	63.96
SChannel I			28	—	62.97
SChannel II			30	—	182.64
OpenSSL-fixed I			32	20	0.02
OpenSSL-fixed II			32	35	83.32
OpenSSL-fixed III			32	35+k	$2^k \cdot 83.32$

On the Practical Exploitability of Dual EC in TLS Implementations

Matt Green, DJB, Tanja Lange et al

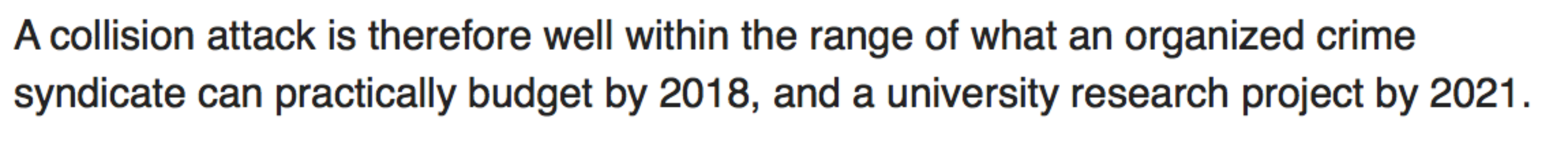
The SHAppening: freestart collisions for SHA-1



cluster with 64 GPUs, or by renting GPU time on Amazon EC2 for about 2K US$.[4] Based on experimental data obtained in this new work and the 2013 state-of-the-art collision attack, we can project that a real SHA-1 collision will take between 49 and 78 days on a 512 GPU cluster. Renting the equivalent GPU time on EC2 will cost between 75K US$ and 120K US$ and will plausibly take at most a few months.

The impact of our work is therefore not only theoretical. Freestart collisions are collisions for SHA-1's compression function, that do not directly translate to collisions for SHA-1, but do directly undermine the security proof of SHA-1. They represent an important alarm signal that warns users to quickly move away from using this hash function. In particular, we believe that our work shows that industry's plan to move away from SHA-1 in 2017 might not be soon enough.

- Freestart collision on full SHA-1 (ePrint 2015/967)



A collision attack is therefore well within the range of what an organized crime syndicate can practically budget by 2018, and a university research project by 2021.

– When Will We See Collisions for SHA-1 (Schneier 2012)

10 second plug

Securi-Tay Information Security conference

https://securi-tay.co.uk

- launched in 2012
- Only Student Led InfoSec Con in UK
- Abertay University, Dundee

- 150 attendees
- 13 talks
- Community sponsors

Conclusions & Questions

Jessy Irwin
@jessysaurusrex

☆｡ 🔐｡ ☆ 🔒
｡ ☆ ｡ ☆｡ ☆
🔑｡ ＼ ｜ ／｡ 🔑
if you like it
then you better
put some crypto
on it
🔑｡ ／ ｜ ＼｡ 🔑
｡ ☆｡ ☆｡ ☆
☆｡ 🔒 ｡ ☆ 🔐