Building trust in an untrustworthy world

Matthew Green
Johns Hopkins University

My background

- Prof. in CS department at JHU
- I work on information security and applied cryptography applied cryptography
- I write a blog (blog.cryptographyengineering.com)
- Co-invented a private cryptocurrency (Zcash) and boy was that weird

This talk

- This is a talk about my last five years of work
- That means I'll have to talk about details a little (but I promise I'll keep the math to a minimum)
- It's also a story about *privacy* and how it's being taken away, sometimes with and without our knowledge

What is cryptography?
(And why should you care?)

CRYPTOQUIP

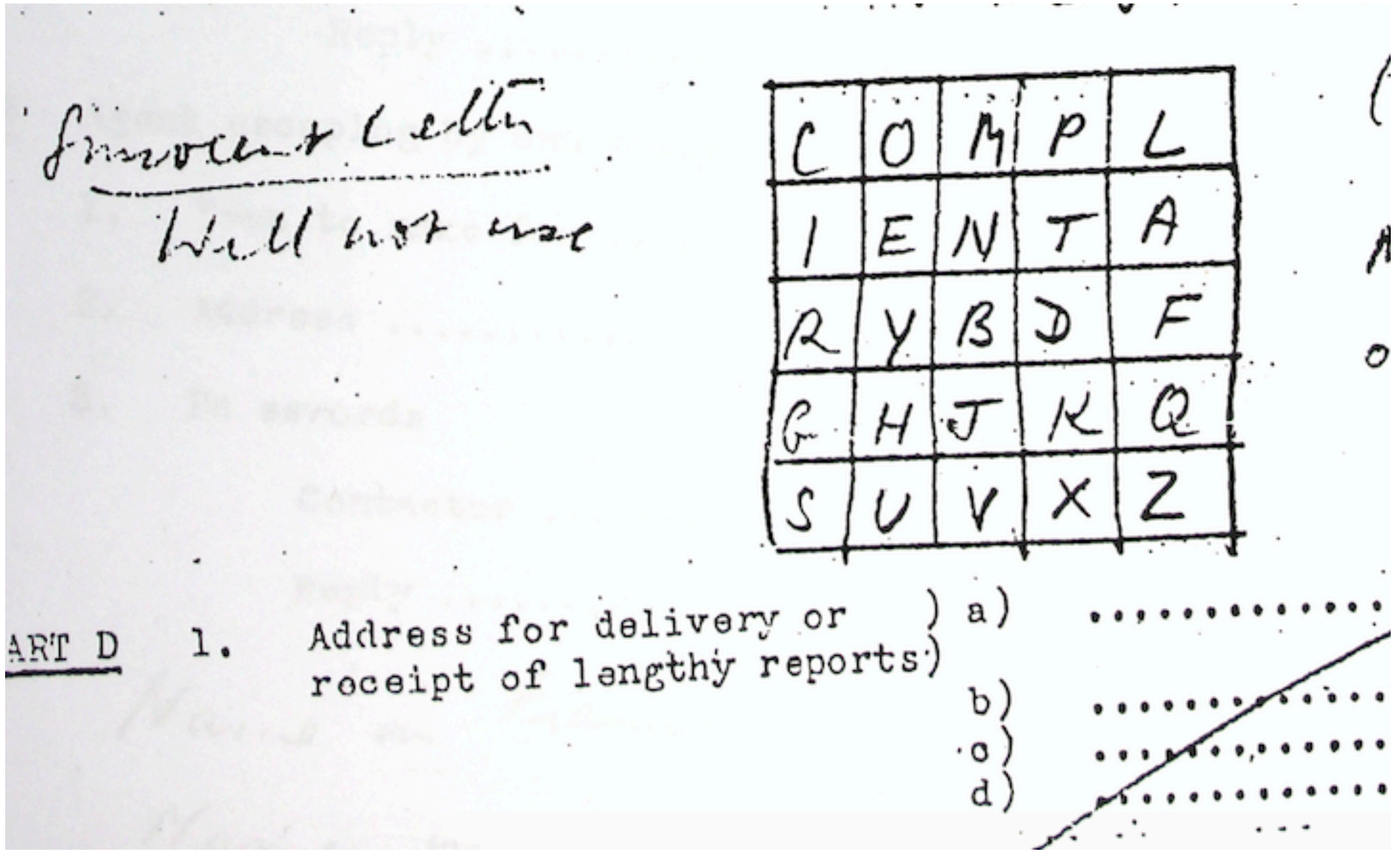
IF A PERSON WERE AN
HK N JUDXQR LUDU NR
EXPERT IN EXAMINING LONG
UIJUDB HR U·INPHRHRW OQRW,
NARROW CRACKS WOULD THAT
RNDDQL ZDNZEX, LQCOM BTNB
MAKE HIM A FISSUREMAN
PNEU THP N KHXXCDUPNR?

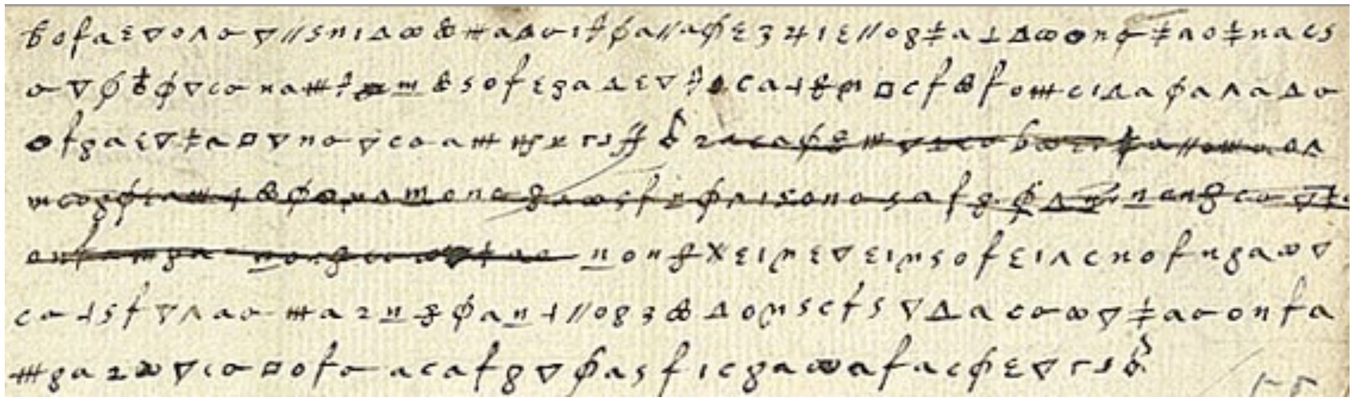
The Cryptoquip is a substitution cipher in which one letter stands for another. If you think X equals O it will equal O throughout the puzzle. Single letters, short words and words using an apostrophe give you clues to locating vowels. Solution is by trial and error.

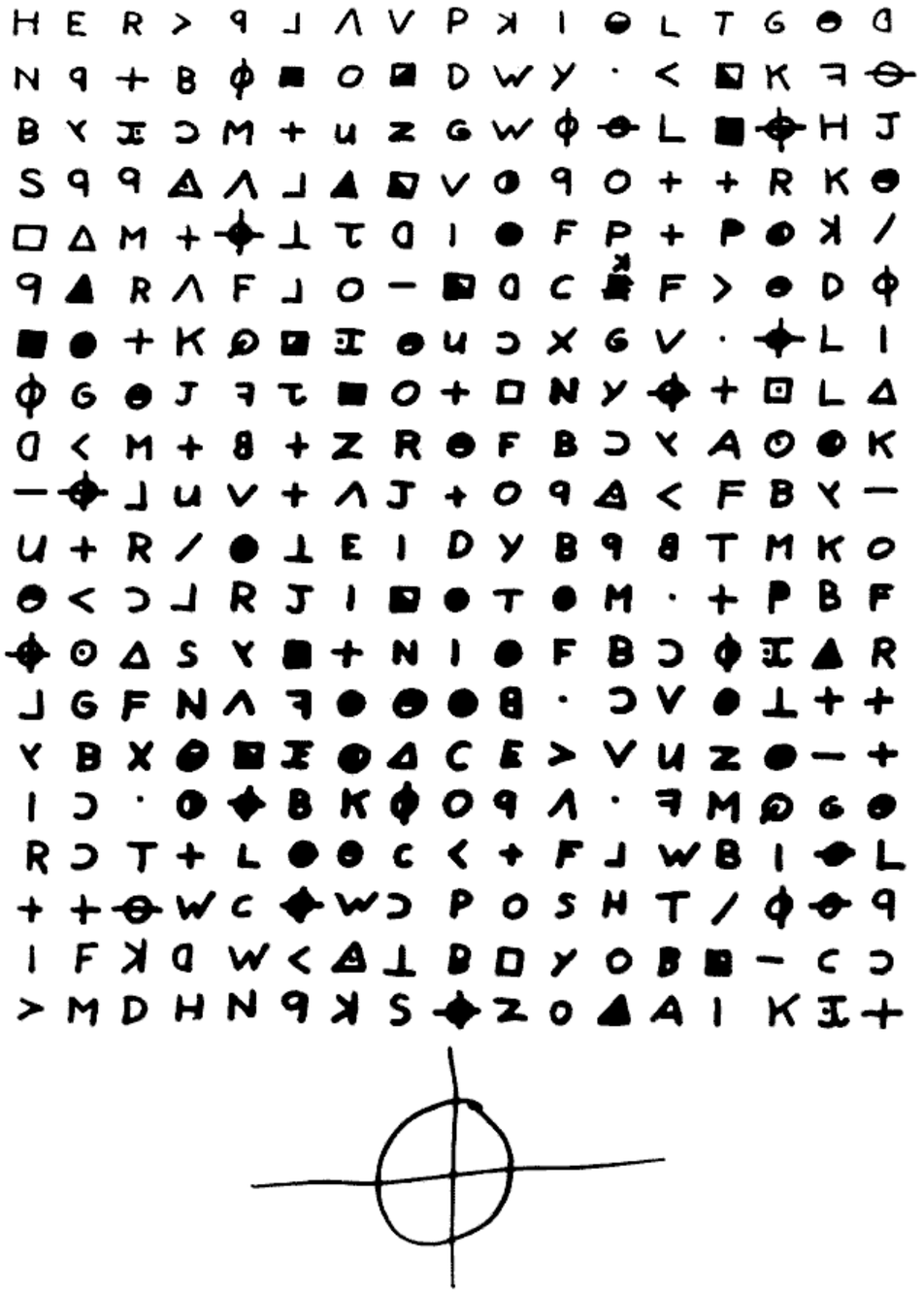
Today's clue: K EQUALS F

YESTERDAY'S CRYPTOQUIP: WHEN MY BROKEN ARM HAD BEEN SET AT THE HOSPITAL, I DECIDED I'D LIKE TO THROW A CAST PARTY.

CROSSWORD PUZZLE *By Dan Naddor*


Innocent Cells
Will not use
C O M P L
I E N T A
R Y B D F
G H J K Q
S U V X Z
ART D 1. Address for delivery or receipt of lengthy reports
a)
b)
c)
d)





I omitted in my late Letters to inform you that the

~~an~~-no-un-ce-d to Do-
Swedish Minister at Versailles had 145.315.772.330.15.4.271.146

c-tor Fra-n-k-li-n the wi-sh of this King to be-com-a
39.209.705.333.129.721.333.6.422.252.94.7.378.271.15.363.4

an ally of the U.States, & treat-y might be with
145.471.94.6.836.53. that the 582.262.317.15. negociated 22.

the Do-c-tor in particular. com-mis-sion has in
6.146.39.209.59.74. A Plenepotentiary 363.724.75.5.59.con

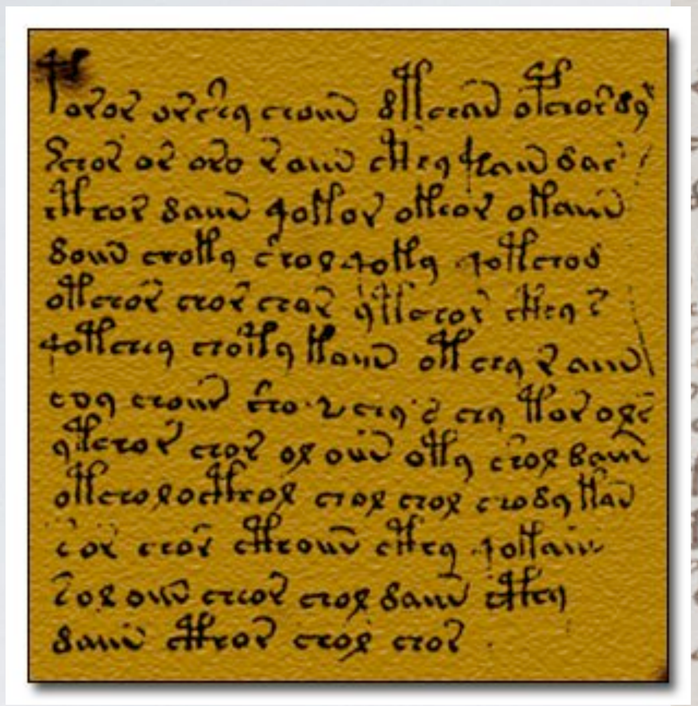
se-que-n-ce is-s-sue-d for that pu-r-pose.
388.575.333.330.443.95.403.47.297.790.781.24.748. The

mo-de-l by Congress i-s pre-t-ty an-
~~[illegible]~~ 737.382.542. transmitted 160.142.443.95.251.48.362.145.

al-o-g-ous to the treat-y with France, li-mi-t-ed
152.69.308.571.271.6.582.262.22.16. but is 721.729.48.47

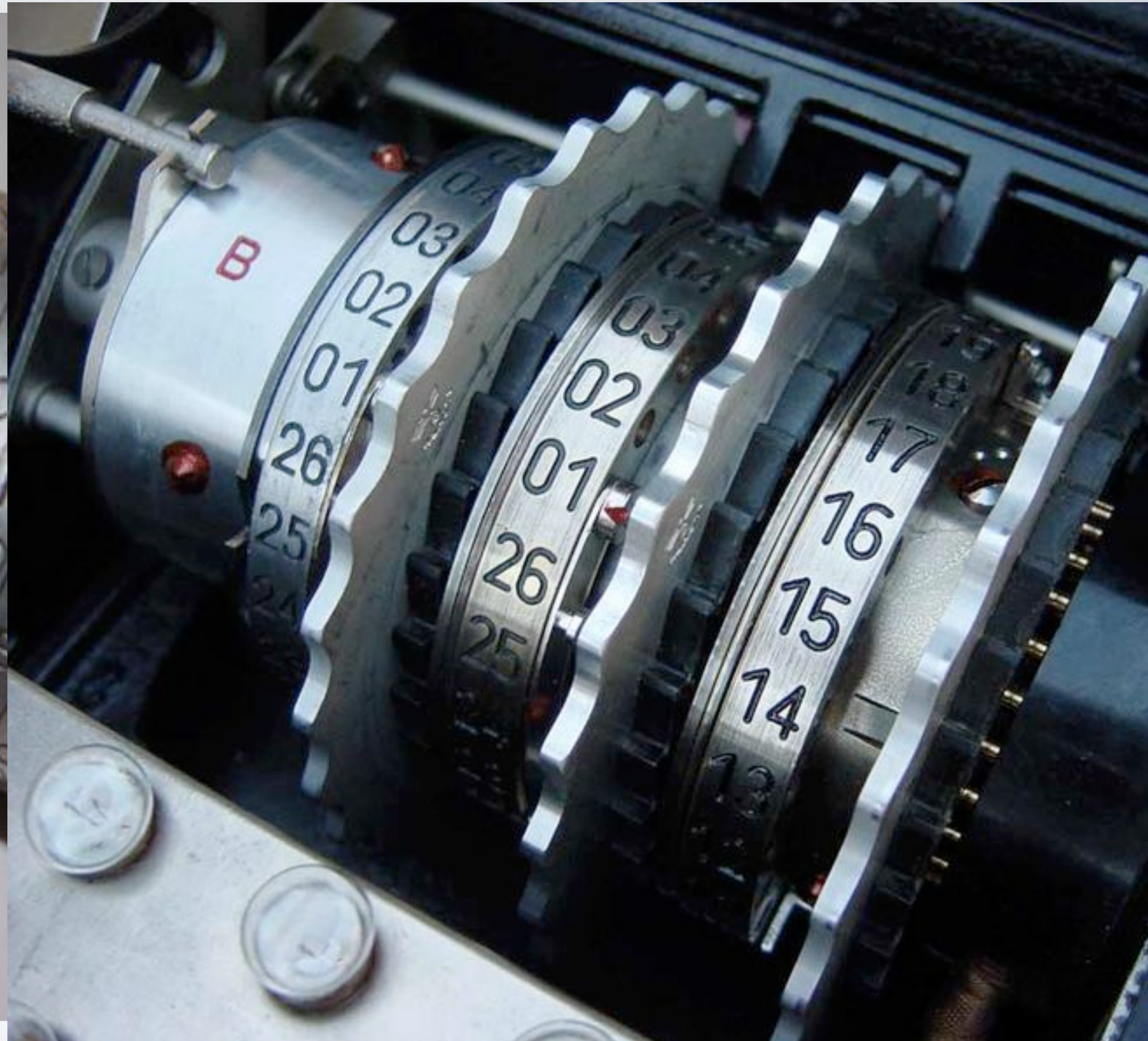
in du-ra-tion to ne-f- ten-year-s.
59.667.616.25.271.731.14.109.244.95.

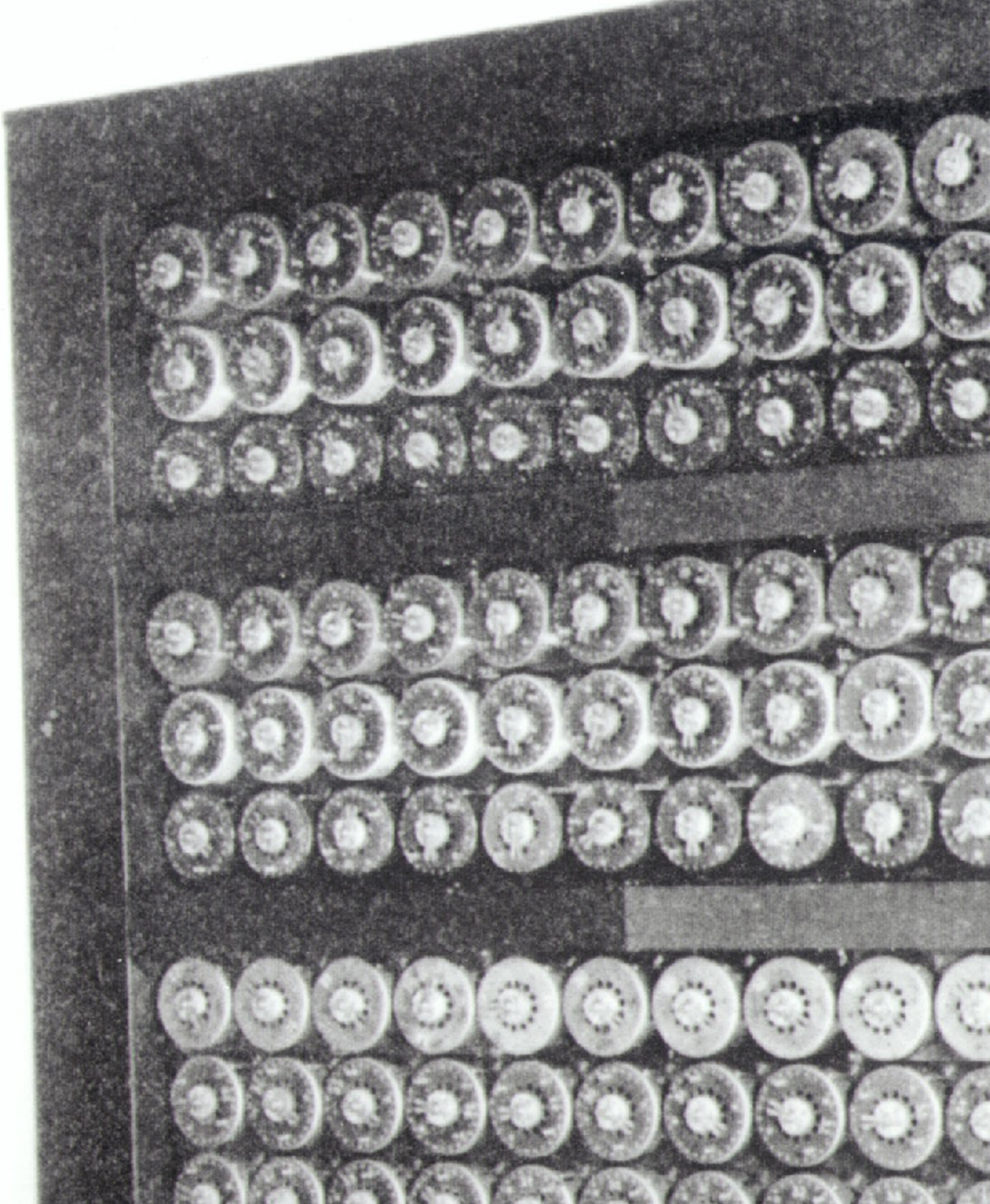
(735fi)



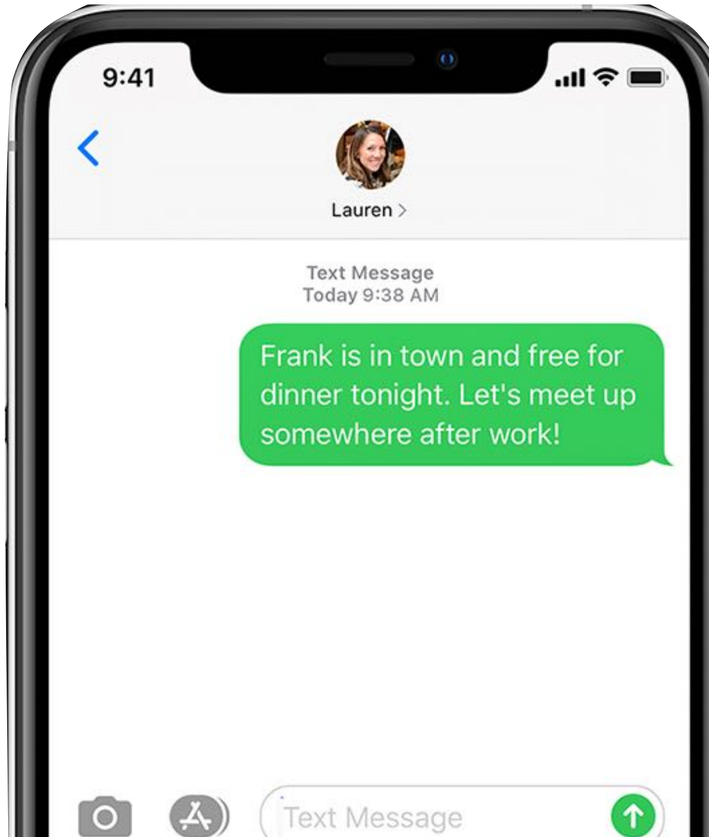

78

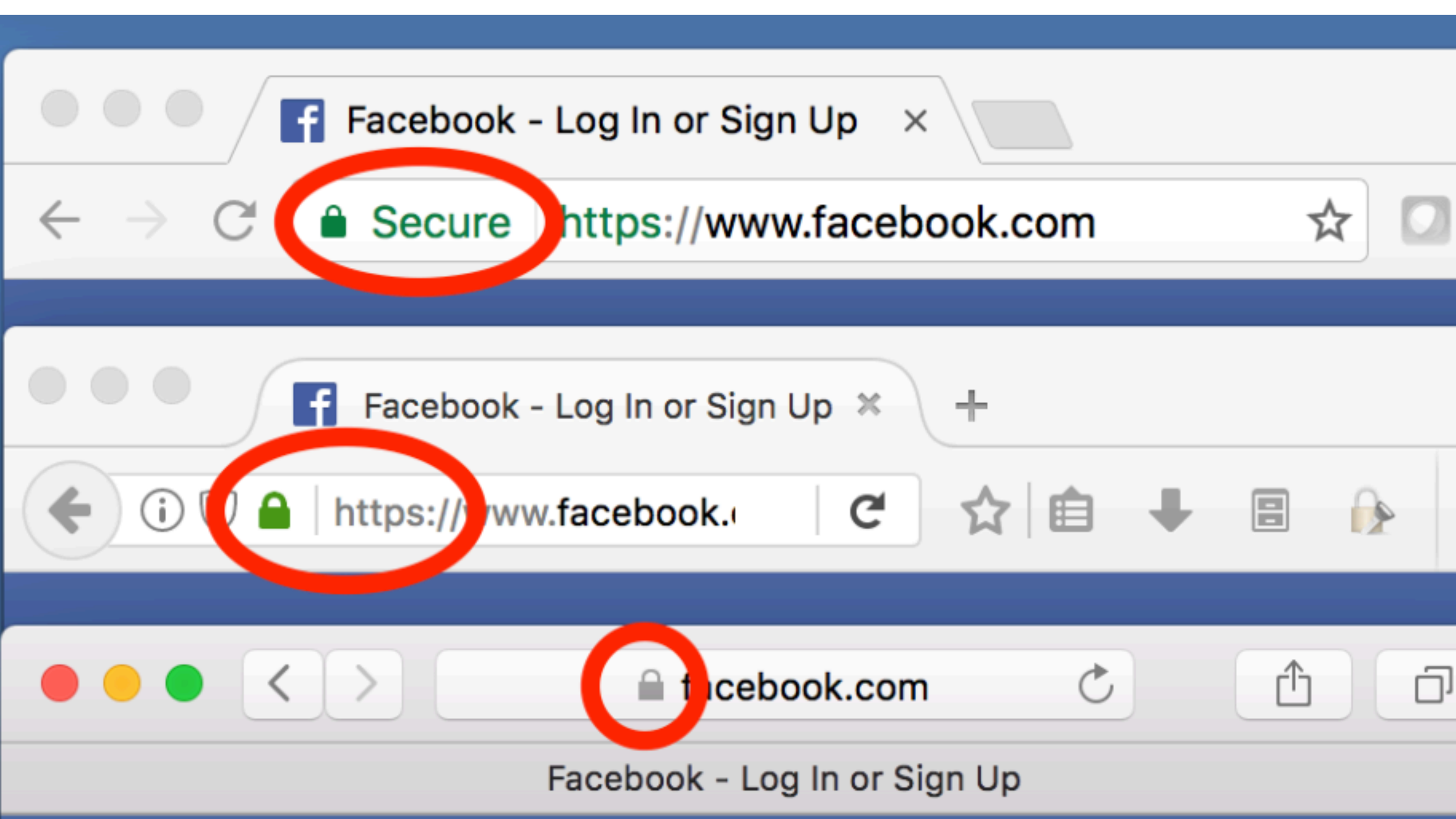

DEVICE
TYPE M-94
NAL CORPS
S. ARMY


B
03
02
01
26
25
03
02
01
26
25
17
16
15
14

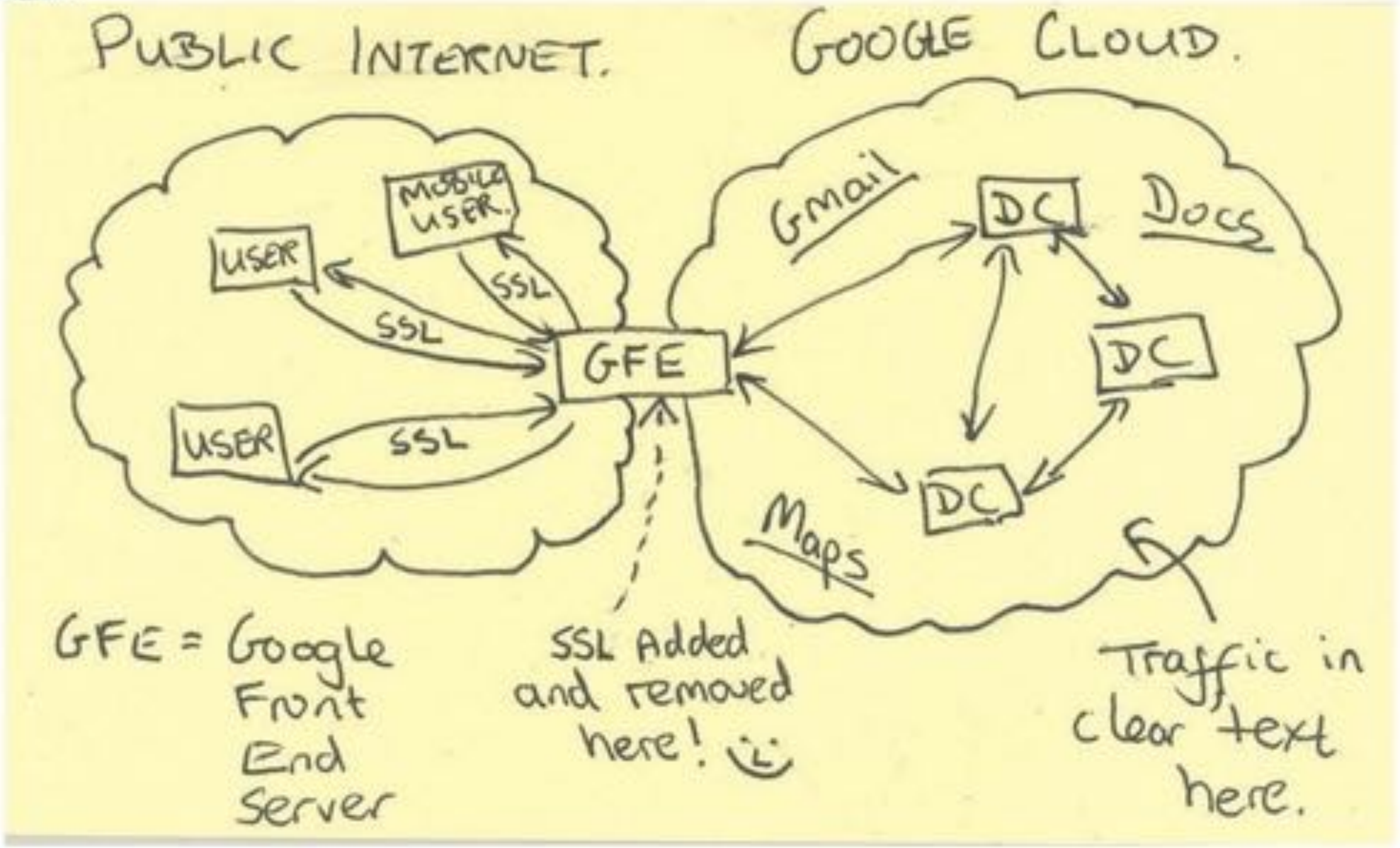



iMessage
Today 9:38 AM
Can I call you back later? I'm at an appointment.
iMessage


9:41
Lauren
Text Message
Today 9:38 AM
Frank is in town and free for dinner tonight. Let's meet up somewhere after work!
Text Message


Facebook - Log In or Sign Up
Secure
https://www.facebook.com
Facebook - Log In or Sign Up
https://www.facebook.
cebook.com
Facebook - Log In or Sign Up

Current Efforts - Google



Download SuperFish Removal Tool

goto fail; // Apple SSL bug test site

This site will help you determine whether your computer is vulnerable to #goto

Tracking the FREAK Attack

QUALYS® SSL LABS

National Security

Johns Hopkins researchers poke a hole in Apple's encryption

This talk:

- **As a society, we depend on encryption to keep our data secure**
  - And thankfully, we've gotten really good at it

This talk:

- **As a society, we depend on encryption to keep our data secure**
  - And thankfully, we've gotten really good at it

Yet all of this progress is based on the assumption that the people who deploy and build those systems are on our side.

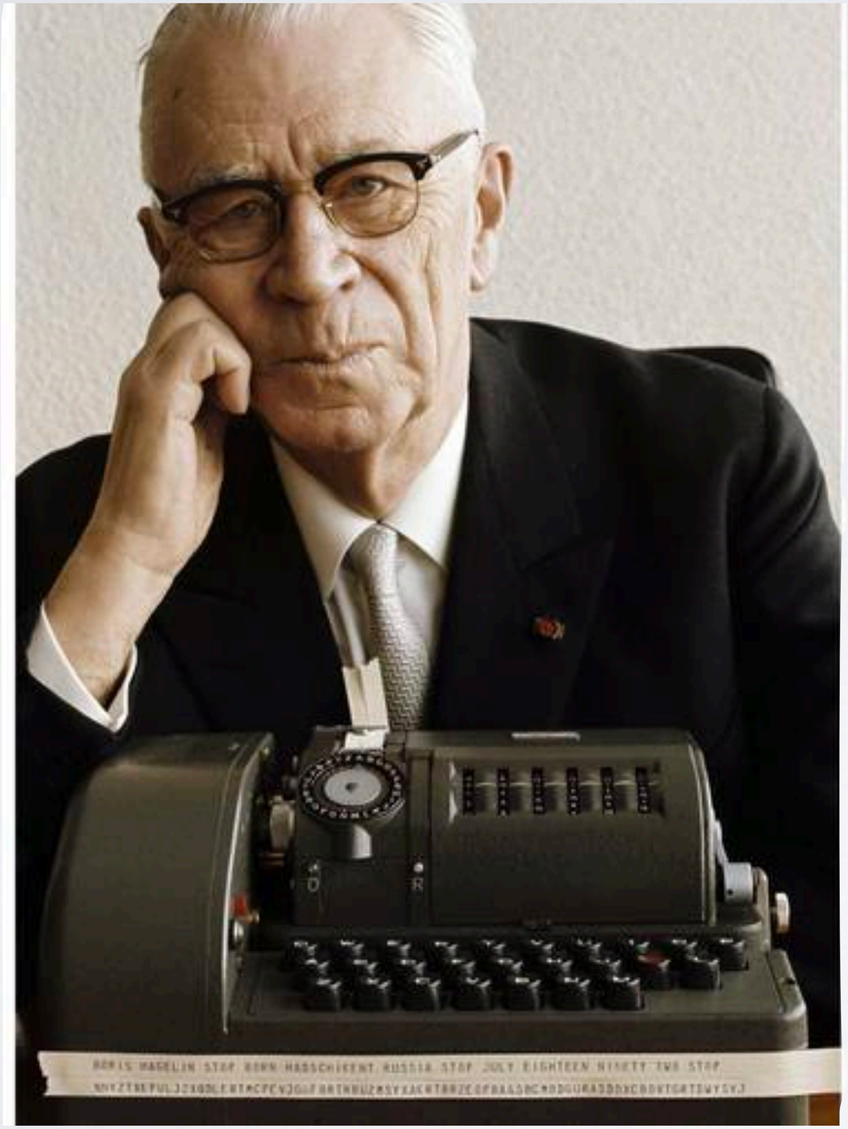
This talk:

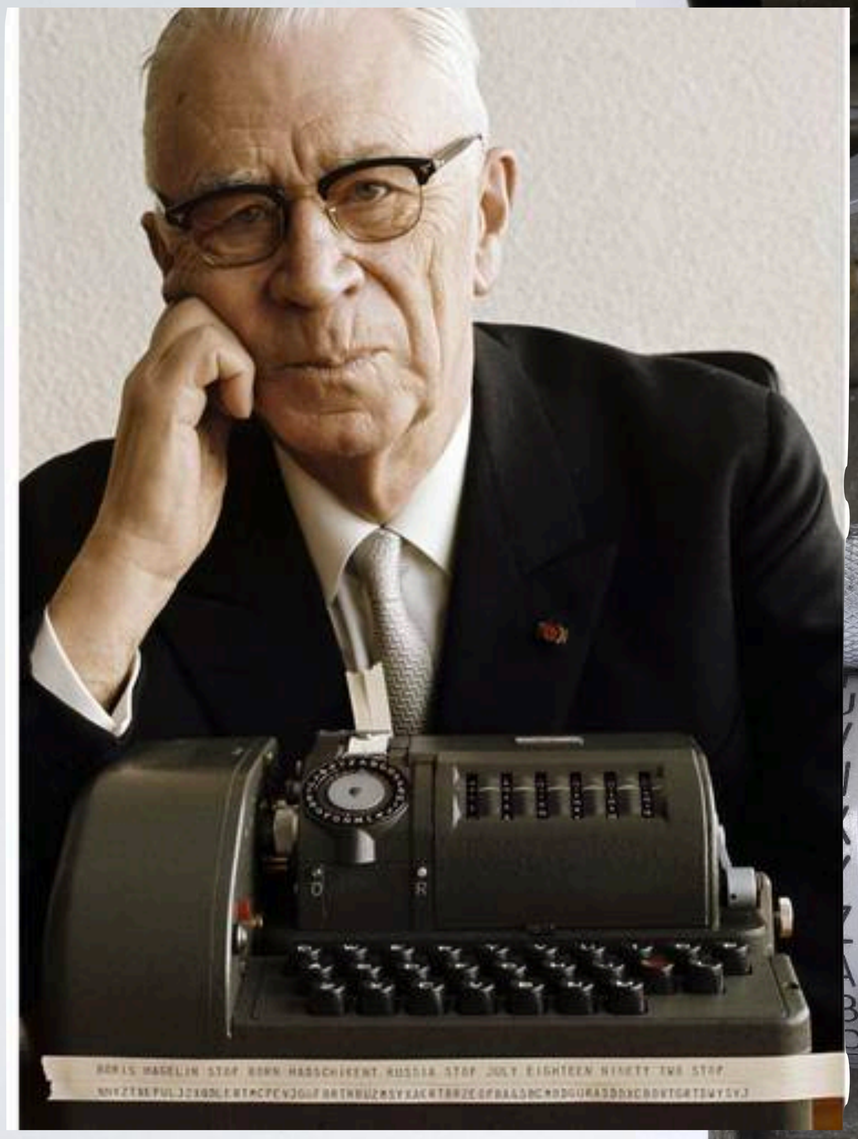
- **As a society, we depend on encryption to keep our data secure**
  - And thankfully, we've gotten really good at it

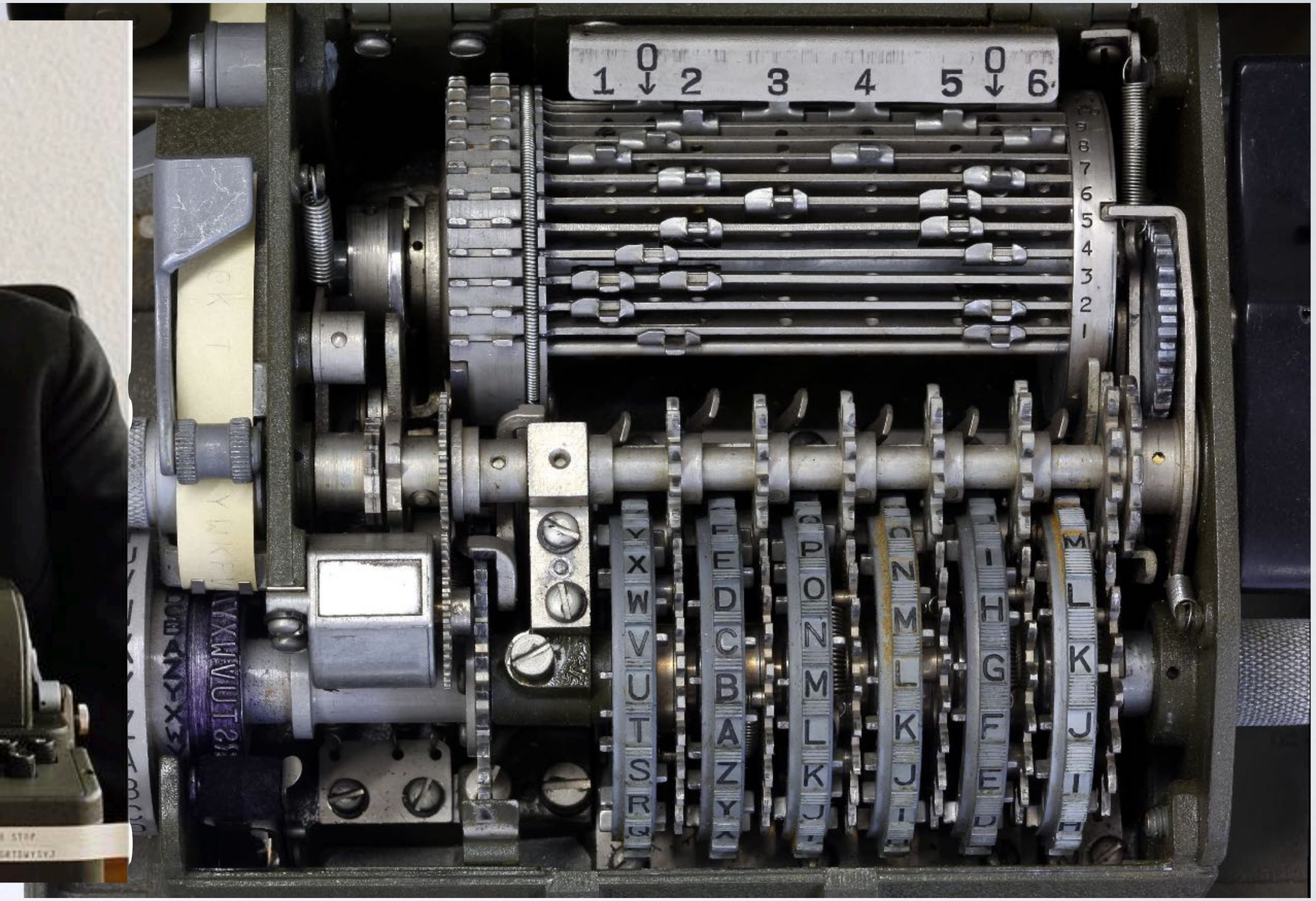
Yet all of this progress is based on the assumption that the people who deploy and build those systems are on our side.

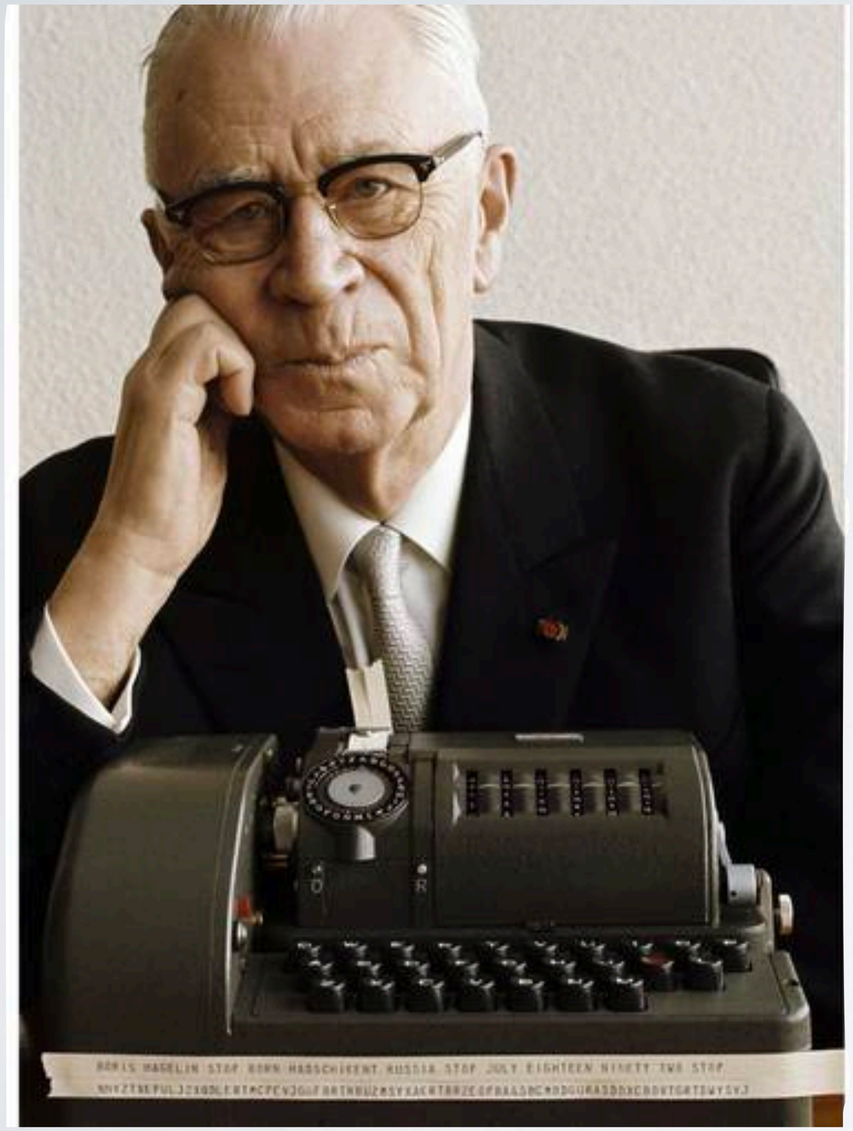
What happens to us if they aren't?

A bit of history (~1930s-1980s)




BERLIN STOP BONN MASCHINENT RUSSIA STOP JULY EIGHTEEN NINETY TWO STOP


0 1 2 3 4 5 0 6
8 7 6 5 4 3 2 1
X W V U T S R
F E D C B A Z Y
P O N M L K J
C M L K J I
I H G F E D
M L K J I



HAGELIN-CRYPTOS

CRYPTO AG

- William F. Friedman (Army SIS, NSA)
  - 1950s: visited Hagelin and son in Zug, Switzerland
  - After his death, papers donated to George C. Marshall foundation. They mention a "gentleman's agreement"
  - NSA requested papers be sequestered in 1976 (accidentally re-opened 1979-1983, then closed again)
  - **In 2015, redacted versions were released to the public**

1. In accordance with Letter Orders 273 dated 27 January 1955, as modified by L.O. 273-A dated 4 February 1955, I left Washington via MATS at 1500 hours on 18 February 1955, arrived at Orly Field, Paris, at 1430 hours on 19 February, and at Zug, Switzerland, at 1830 the same day. I spent the next few days with Mr. Boris C.W. Hagelin, Senior, and Mr. Boris Hagelin, Junior, for the purpose of learning the status of their new developments in crypto-apparatus and of making an approach and a proposal to Mr. Hagelin, Senior as was recently authorized by USCIB and concurred in by LSIB. Upon completion of that part of my mission, I left Zug at 1400 hours on 28 February and proceeded to London, arriving at 1845 that evening.

1. In accordance with Letter Orders 273 dated 27 January 1955, as modified by L.O. 273-A dated 4 February 1955, I left Washington via MATS at 1500 hours on 18 February 1955, arrived at Orly Field, Paris, at 1430 hours on 19 February, and at Zug, Switzerland, at 1830 the same day. I spent the next few days with Mr. Boris C.W. Hagelin, Senior, and Mr. Boris Hagelin, Junior, for the purpose of learning the status of their new developments in crypto-apparatus and

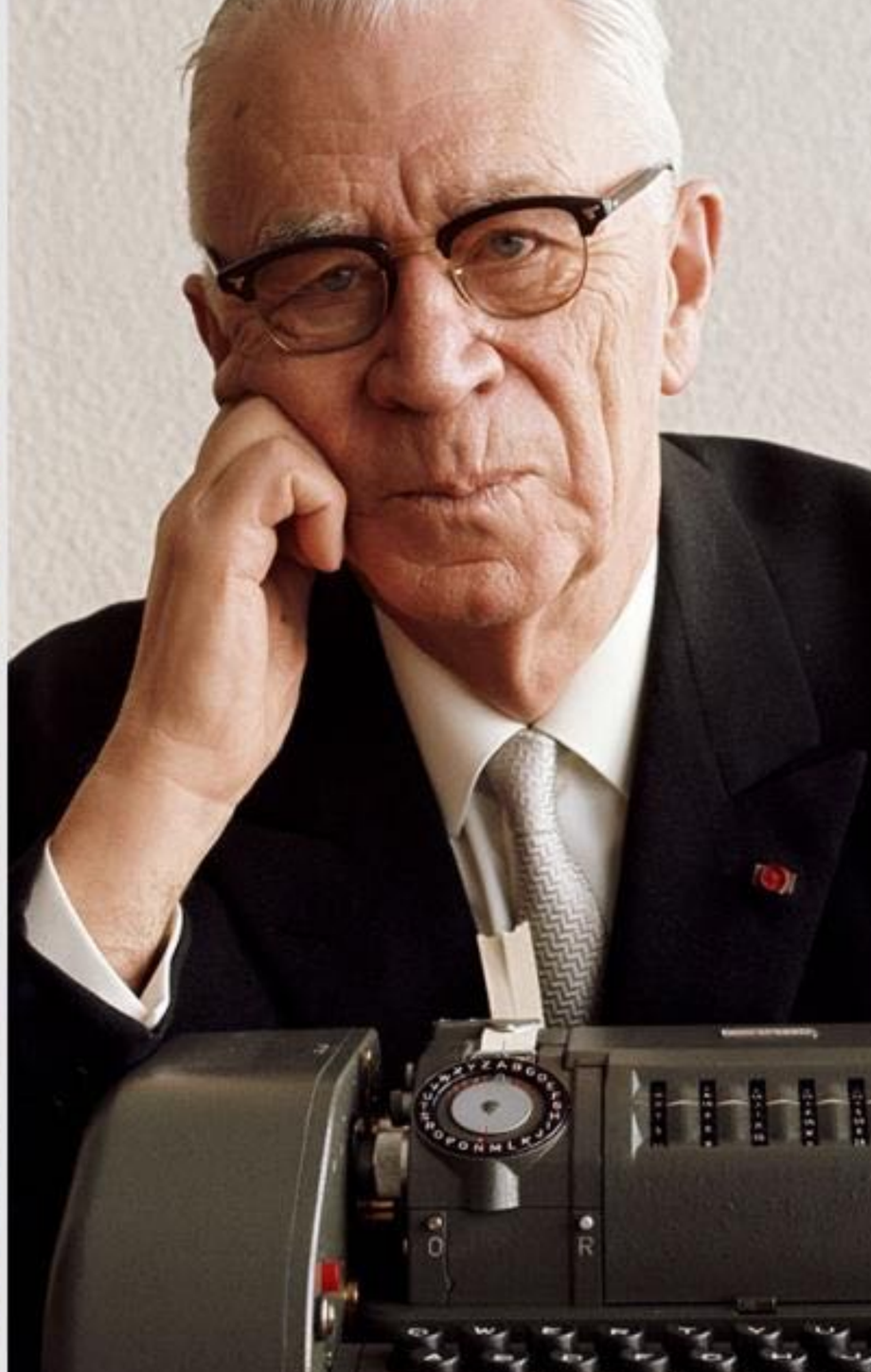
Upon completion of that part of my mission, I left Zug at 1400 hours on 28 February and proceeded to London, arriving at 1845 that evening.

(3) Hagelin Junior was so enthusiastic about this new model that within two or three minutes immediately following our initial exchange of greetings he announced that they had decided to stop making the CX model and are switching over to a variation of the C-52 which, he said, "is simpler in mechanical effectuation and more readily adaptable to the crypto-control mechanism for the HX or electrical-rotor machine." I was, of course, rather startled by this statement and later queried Hagelin Senior about it, saying that I was astonished at the decision to switch to the C-52Y before any security evaluation at all had been made of it. Hagelin Senior said, "Oh, Bo is young and overflowing with enthusiasm. We will hold up making that model if you want us to hold up on it." I told him that I thought this might be advisable, and that in any case we would want one of these models just as soon as possible. Hagelin Senior said that it was easy to convert a

~~TOP SECRET~~

(3) Hagelin Junior was so enthusiastic about this new model that within two or three minutes immediately following our initial exchange of greetings he announced that they had decided to stop making the CX model and are switching over to a variation of the C-52 which, he said, "is simpler in mechanical effectuation and more readily adaptable to the crypto-control mechanism for the HX or electrical-rotor machine." I was, of course, rather startled by this statement and later queried Hagelin Senior about it, saying that I was astonished at the decision to switch to the C-52Y before any security evaluation at all had been made of it. Hagelin Senior said, "Oh, Bo is young and overflowing with enthusiasm.

Hagelin Senior said that it was easy to convert a



- In the 1980s, Iran arrested Crypto AG's representative Hans Buhler on suspicion that the company's machines were backdoor
- The company denied everything, paid a $1m ransom, then charged it to Buhler
- Buhler and other employees went to the press, providing a stream of accusations of government collusion that destroyed the company
- Crypto AG was saved from bankruptcy by "angel investor" Marc Rich

The New York Times

Secret Documents Reveal N.S.A. Campaign Against Encryption

Documents show that the N.S.A. has been waging a war against encryption using a battery of methods that include working with industry to weaken encryption standards, making design changes to cryptographic software, and pushing international encryption standards it knows it can break. Related Article »

Excerpt from 2013 Intelligence Budget Request | Bullrun Briefing Sheet

This excerpt from the N.S.A.'s 2013 budget request outlines the ways in which the agency circumvents the encryption protection of everyday Internet communications. The Sigint Enabling Project involves industry relationships, clandestine changes to commercial software to weaken encryption, and lobbying for encryption standards it can crack.

Source: NYT/ProPublica

TOP SECRET//SI/TK//NOFORN

(U) COMPUTER NETWORK OPERATIONS
(U) SIGINT ENABLING

(U) Project Description

(TS//SI//NF) The SIGINT Enabling Project actively engages the US and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs. These design changes make the systems in question exploitable through SIGINT collection (e.g., Endpoint, MidPoint, etc.) with foreknowledge of the modification. To the consumer and other adversaries, however, the systems' security remains intact. In this

- (TS//SI//NF) Shape the worldwide commercial cryptography marketplace to make it more tractable to advanced cryptanalytic capabilities being developed by NSA/CSS. [CCP_00090]

- (TS//SI//REL TO USA, FVEY) Insert vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets.
- (TS//SI//REL TO USA, FVEY) Collect target network data and metadata via cooperative network carriers and/or increased control over core networks.
- (TS//SI//REL TO USA, FVEY) Leverage commercial capabilities to remotely deliver or receive information to and from target endpoints.
- (TS//SI//REL TO USA, FVEY) Exploit foreign trusted computing platforms and technologies.
- (TS//SI//REL TO USA, FVEY) Influence policies, standards and specification for commercial public key technologies.

TOP SECRET//SI/TK//NOFORN

(U) COMPUTER NETWORK OPERATIONS
(U) SIGINT ENABLING

Source: NYT/ProPublica

(U) Project Description

(TS//SI//NF) The SIGINT Enabling Project actively engages the US and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs. These design changes make the systems in question exploitable through SIGINT collection (e.g., Endpoint, MidPoint, etc.) with foreknowledge of the modification. To the consumer and other adversaries, however, the systems' security remains intact. In this

- (TS//SI//NF) Shape the worldwide commercial cryptography marketplace to make it more tractable to advanced cryptanalytic capabilities being developed by NSA/CSS. [CCP_00090]

- (TS//SI//REL TO USA, FVEY) Insert vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets.

Insert vulnerabilities into commercial encryption systems, IT systems,

- (TS//SI//REL TO USA, FVEY) Influence policies, standards and specification for commercial public key technologies.

Source: NYT/ProPublica

TOP SECRET//SI/TK//NOFORN

(U) COMPUTER NETWORK OPERATIONS
(U) SIGINT ENABLING

(U) Project Description

(TS//SI//NF) The SIGINT Enabling Project actively engages the US and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs. These design changes make the systems in question exploitable through SIGINT collection (e.g., Endpoint, MidPoint, etc.) with foreknowledge of the modification. To the consumer and other adversaries, however, the systems' security remains intact. In this

- (TS//SI//NF) Shape the worldwide commercial cryptography marketplace to make it more tractable to advanced cryptanalytic capabilities being developed by NSA/CSS. [CCP_00090]

- (TS//SI//REL TO USA, FVEY) Insert vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets.
- (TS//SI//REL TO USA, FVEY) Collect target network data and metadata via cooperative network carriers

Influence policies, standards and specification for commercial public key technologies.

- (TS//SI//REL TO USA, FVEY) Influence policies, standards and specification for commercial public key technologies.

Source: NYT/ProPublica

TOP SECRET//SI/TK//NOFORN

(U) COMPUTER NETWORK OPERATIONS
(U) SIGINT ENABLING

(U) Project Description

(TS//SI//NF) The SIGINT Enabling Project actively engages the US and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs. These design changes make the systems in question exploitable through SIGINT collection (e.g., Endpoint, MidPoint, etc.) with foreknowledge of the modification. To the consumer and other adversaries, however, the systems' security remains intact. In this

- (TS//SI//NF) Shape the worldwide commercial cryptography marketplace to make it more tractable to advanced cryptanalytic capabilities being developed by NSA/CSS. [CCP_00090]

To the consumer and other adversaries, however, the systems' security remains intact.

and/or increased control over core networks.

- (TS//SI//REL TO USA, FVEY) Leverage commercial capabilities to remotely deliver or receive information to and from target endpoints.
- (TS//SI//REL TO USA, FVEY) Exploit foreign trusted computing platforms and technologies.
- (TS//SI//REL TO USA, FVEY) Influence policies, standards and specification for commercial public key technologies.

- The Snowden leaks told us what was happening
  - **But they didn't tell us how**
  - **They did leave us a pointer, though**

NIST Special Publication 800-90A

Recommendation for Random Number Generation Using Deterministic Random Bit Generators

ISO/IEC 18031:2011

Information technology -- Security techniques -- Random bit generation

10.3.1 Dual Elliptic Curve Deterministic RBG (Dual_EC_DRBG)

Dual_EC_DRBG is based on the following hard problem, sometimes known as the "elliptic curve discrete logarithm problem" (ECDLP): given points P and Q on an elliptic curve of order n, find a such that $Q = aP$.

Achilles heel: randomness

- **Many protocols, one commonality:**
  - Most cryptographic protocols devour random bits
    - Ex: 108 bytes / TLS session
  - The quality of those bits is hugely important
  - Attacker who can predict random number generator output can break (almost) any cryptographic system

RNG System Architecture (1)

TRNG

bits

Crypto Protocols

(SSL, TLS, IPSec, etc.)

Probabilistic:
system specific, hardware/entropy collection

RNG System Architecture (2)

seed

bits

Crypto Protocols

(SSL, TLS, IPSec, etc.)

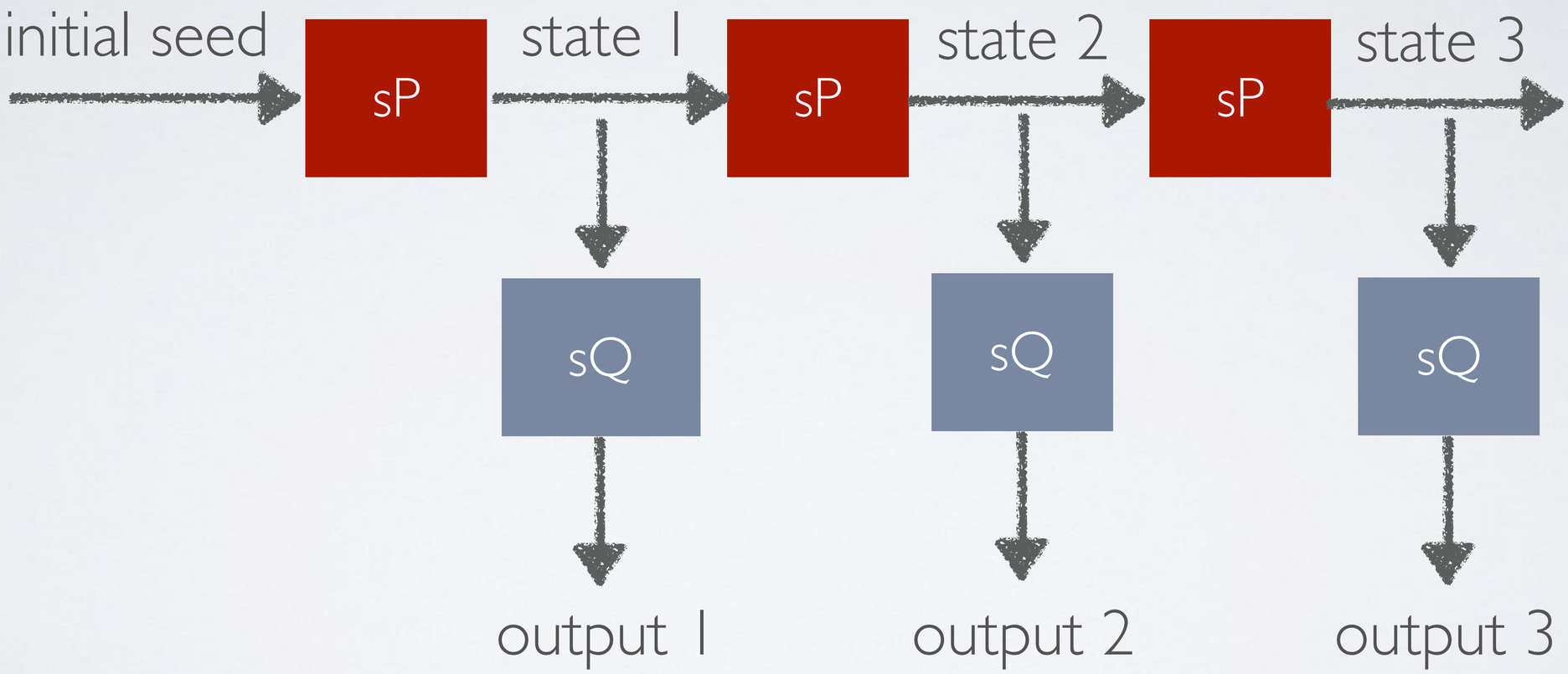
TRNG

PRNG (DRBG)

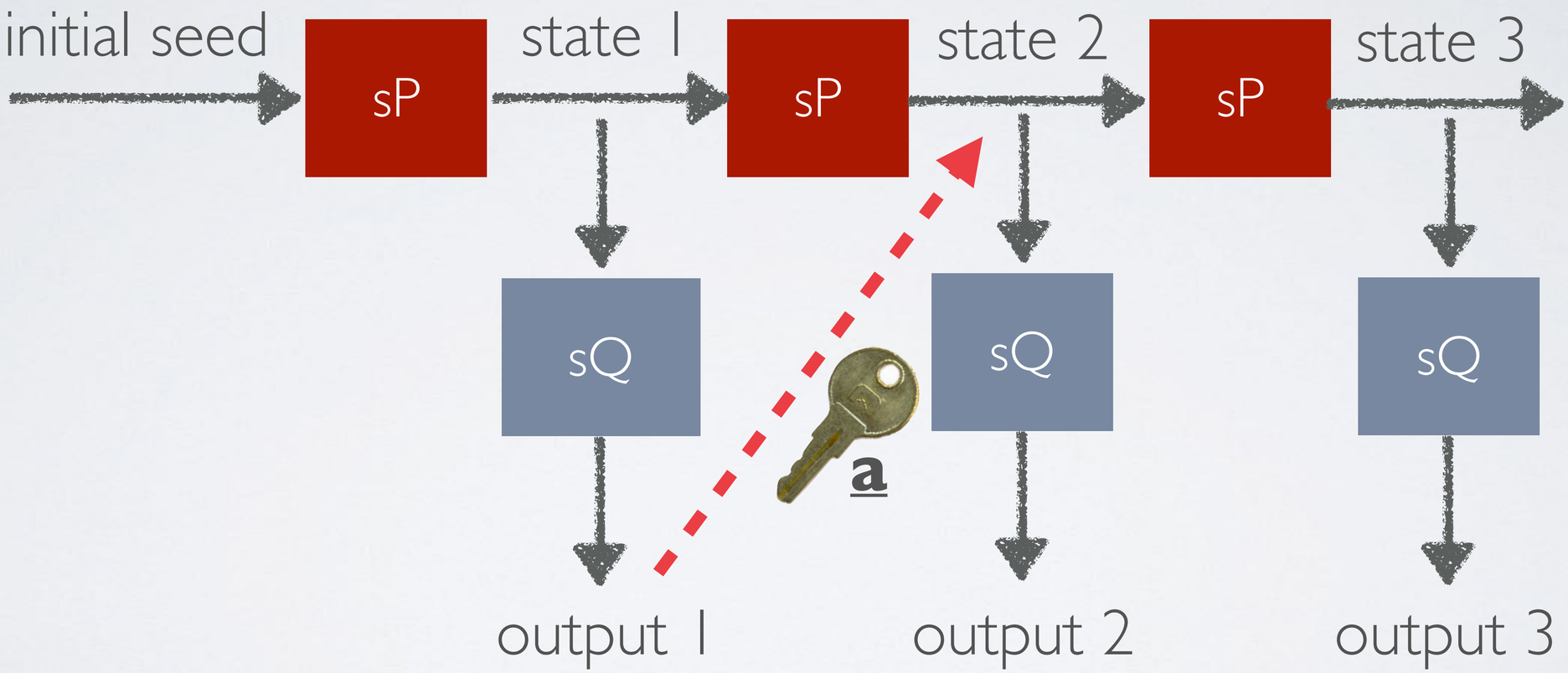
Probabilistic:
system specific, hardware, entropy collection

Deterministic:
computational, fast, algorithmic

Dual EC (NSA, late 1990s)



Dual EC



If P = aQ: sP = a(sQ)

Shumow & Ferguson / CRYPTO 2007

- **What we learned:**
  - There was a flaw in a widely-used US standard cryptographic algorithm
  - Someone who made that algorithm (and picked a value "Q") could know a "backdoor" that breaks any system based on it
  - So: who made Q?

Who made the master key?

-----Original Message-----
From: John Kelsey [mailto:john.kelsey@nist.gov]
Sent: Wednesday, October 27, 2004 11:17 AM
To: Don Johnson
Subject: Minding our Ps and Qs in Dual_EC

Do you know where Q comes from in Dual_EC_DRBG?

Thanks,

-John

Source: NIST FOIA

Who made the master key?

Subject: RE: Minding our Ps and Qs in Dual_EC
From: "Don Johnson" <DJohnson@cygnacom.com>
Date: Wed, October 27, 2004 11:42 am
To: "John Kelsey" <john.kelsey@nist.gov>

John,

P = G.
Q is (in essence) the public key for some random private key.

It could also be generated like a(nother) canonical G, but NSA kyboshed this idea, and I was not allowed to publicly discuss it, just in case you may think of going there.

Don B. Johnson

Source: NIST FOIA

Fast forward to 2015

Juniper is committed to maintaining the integrity and security of our products and wanted to make customers aware of critical patched releases we are issuing today to address vulnerabilities in devices running ScreenOS® software.

During a recent internal code review, Juniper discovered unauthorized code in ScreenOS that could allow a knowledgeable attacker to gain administrative access to NetScreen® devices and to decrypt VPN connections. Once we identified these vulnerabilities, we launched an investigation into the matter, and worked to develop and issue patched releases for the latest versions of ScreenOS.

At this time, we have not received any reports of these vulnerabilities being exploited; however, we strongly recommend that customers update their systems and apply the patched releases with the highest priority.

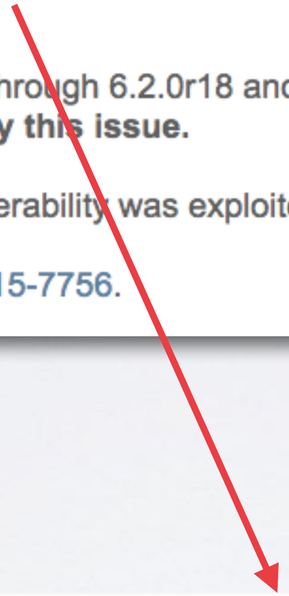
CVE-2015-**7756**

VPN Decryption (CVE-2015-7756) may allow a knowledgeable attacker who can monitor VPN traffic to decrypt that traffic. It is independent of the first issue.

This issue affects ScreenOS 6.2.0r15 through 6.2.0r18 and 6.3.0r12 through 6.3.0r20. **No other Juniper products or versions of ScreenOS are affected by this issue.**

There is no way to detect that this vulnerability was exploited.

This issue has been assigned CVE-2015-7756.



VPN Decryption (CVE-2015-7756) may allow a knowledgeable attacker who can monitor VPN traffic to decrypt that traffic.

Vulnerable -> Patched

ScreenOS 6.3.0r20
(vulnerable)

```
2551....9585320EEAF81044F20D5503
0A035B11BECE81C785E6C933E4A8A131
F6578107....interrupt disabled a
2551....2c55e5e45edf713dc43475ef
fe8813a60326a64d9ba3d2e39cb639b0
f3b0ad10....interrupt disabled a
```

ScreenOS 6.3.0r21
(patched)

Sources: Adam Caudill, Peter Bowen, HD Moore, Ralf Phillip Weinmann

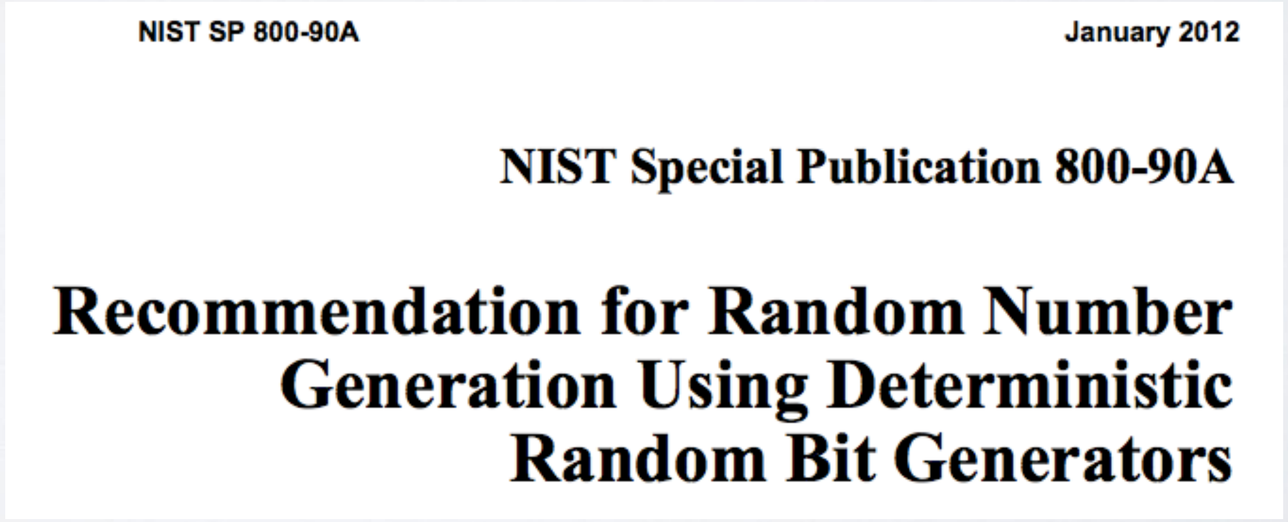
Dual EC DRBG

P-256 Weierstraß *b*

P-256 *P* x coord

P-256 field order

```
    5AC635D8AA3A93E7B3EBBD55769886BC651D06B                C3E27D2604B
    6B17D1F2E12C4247F8BCE6E563A440F277037D812DEB33A0F4A139
    FFFFFFFF00000000FFFFFFFFFFFFFFFFBCE6FAADA7179E84F3B9CAC2FC632551
bad: 9585320EEAF81044F20D55030A035B11BECE81C785E6C933E4A8A131F6578107
good:2c55e5e45edf713dc43475effe8813a60326a64d9ba3d2e39cb639b0f3b0ad10
nist:c97445f45cdef9f0d3e05e1e585fc297235b82b5be8ff3efca67c59852018192
```



NIST SP 800-90A January 2012

NIST Special Publication 800-90A

Recommendation for Random Number Generation Using Deterministic Random Bit Generators

FIPS Approved Algorithms

The following FIPS approved algorithms are supporte

- DSA , ECDSA Sign Verify
- SHA-1, SHA-256
- Triple-DES (CBC)

Juniper Networks SSG 5 and SSG 20 Security Policy

FIPS 140-2 SECURITY POLICY

Juniper Networks, Inc.

SSG 5 and SSG 20

HW P/N SSG-5 and SSG-20, FW Version ScreenOS 6.2.0

Document # 530-023728-01

- AES (CBC)
- HMAC-SHA-1, HMAC-SHA-256
- RSA Sign/Verify (PKCS #1)
- ANSI X9.31 DRNG

Juniper doesn't appear to use Dual EC...

Dual EC in ScreenOS

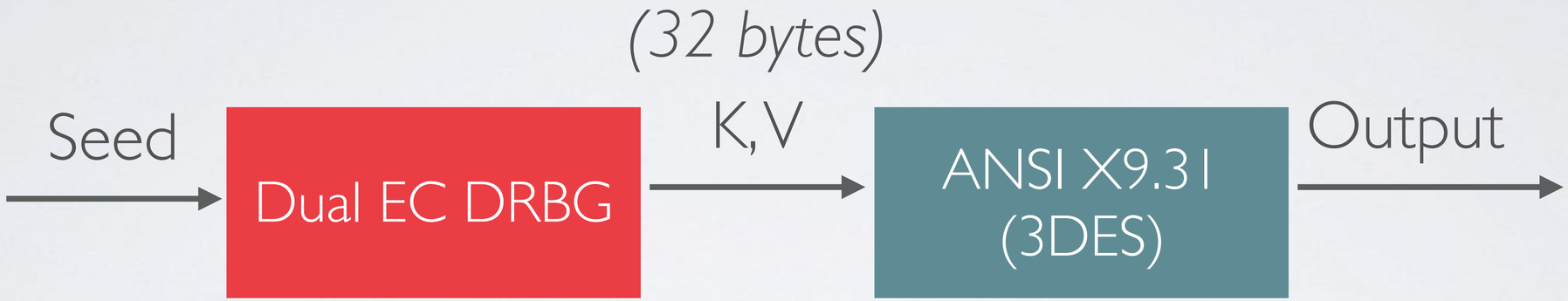
The following product families do utilize Dual_EC_DRBG, but do not use the pre-defined points cited by NIST:

1. ScreenOS*

*ScreenOS does make use of the Dual_EC_DRBG standard, but is designed to not use Dual_EC_DRBG as its primary random number generator. ScreenOS uses it in a way that should not be vulnerable to the possible issue that has been brought to light. Instead of using the NIST recommended curve points it uses self-generated basis points and then takes the output as an input to FIPS/ANSI X.9.31 PRNG, which is the random number generator used in ScreenOS cryptographic operations.

“ScreenOS does make use of the Dual_EC_DRBG standard, but is designed not to use Dual_EC_DRBG as its primary random number generator. ScreenOS uses it it in a way that shouldn't be vulnerable to the possible issue that has been brought to light.” (2013)

RNG Cascade



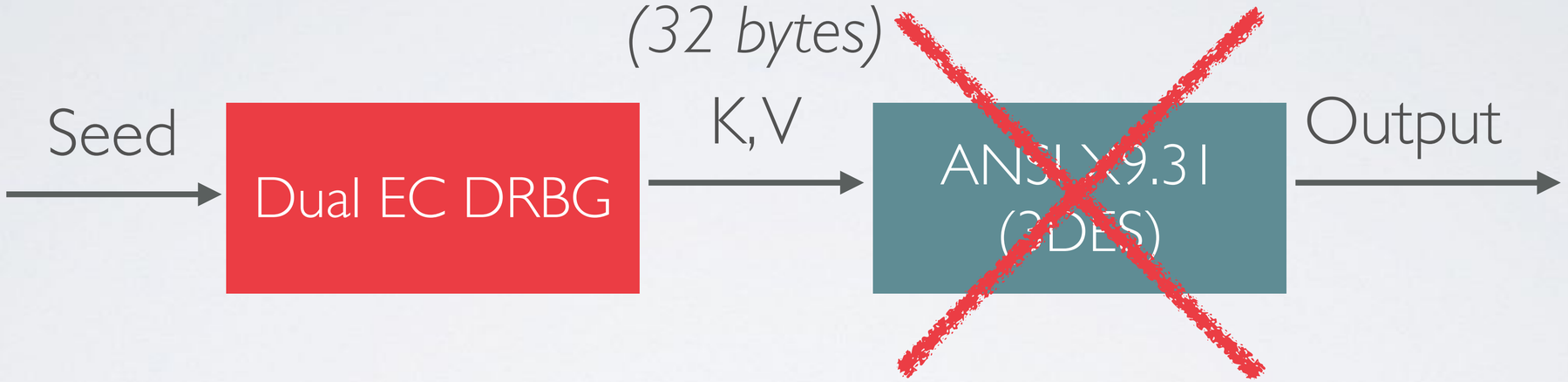
This approach *should* neutralize any backdoor

```
1  void prng_reseed(void) {
2    blocks_generated_since_reseed = 0;
3    if (dualec_generate(prng_temporary, 32) != 32)
4      error_handler("FIPS ERROR: PRNG failure, unable to reseed\n", 11);
5    memcpy(prng_seed, prng_temporary, 8);
6    prng_output_index = 8;
7    memcpy(prng_key, &prng_temporary[prng_output_index], 24);
8    prng_output_index = 32;
9  }
10 void prng_generate(void) {
11   int time[2];
12
13   time[0] = 0;
14   time[1] = get_cycles();
15   prng_output_index = 0;
16   ++blocks_generated_since_reseed;
17   if (!one_stage_rng())
18     prng_reseed();
19   for (; prng_output_index <= 0x1F; prng_output_index += 8) {
20     // FIPS checks removed for clarity
21     x9_31_generate_block(time, prng_seed, prng_key, prng_block);
22     // FIPS checks removed for clarity
23     memcpy(&prng_temporary[prng_output_index], prng_block, 8);
24   }
25 }
```

ANSI generator is never run.
Dual EC output emitted.

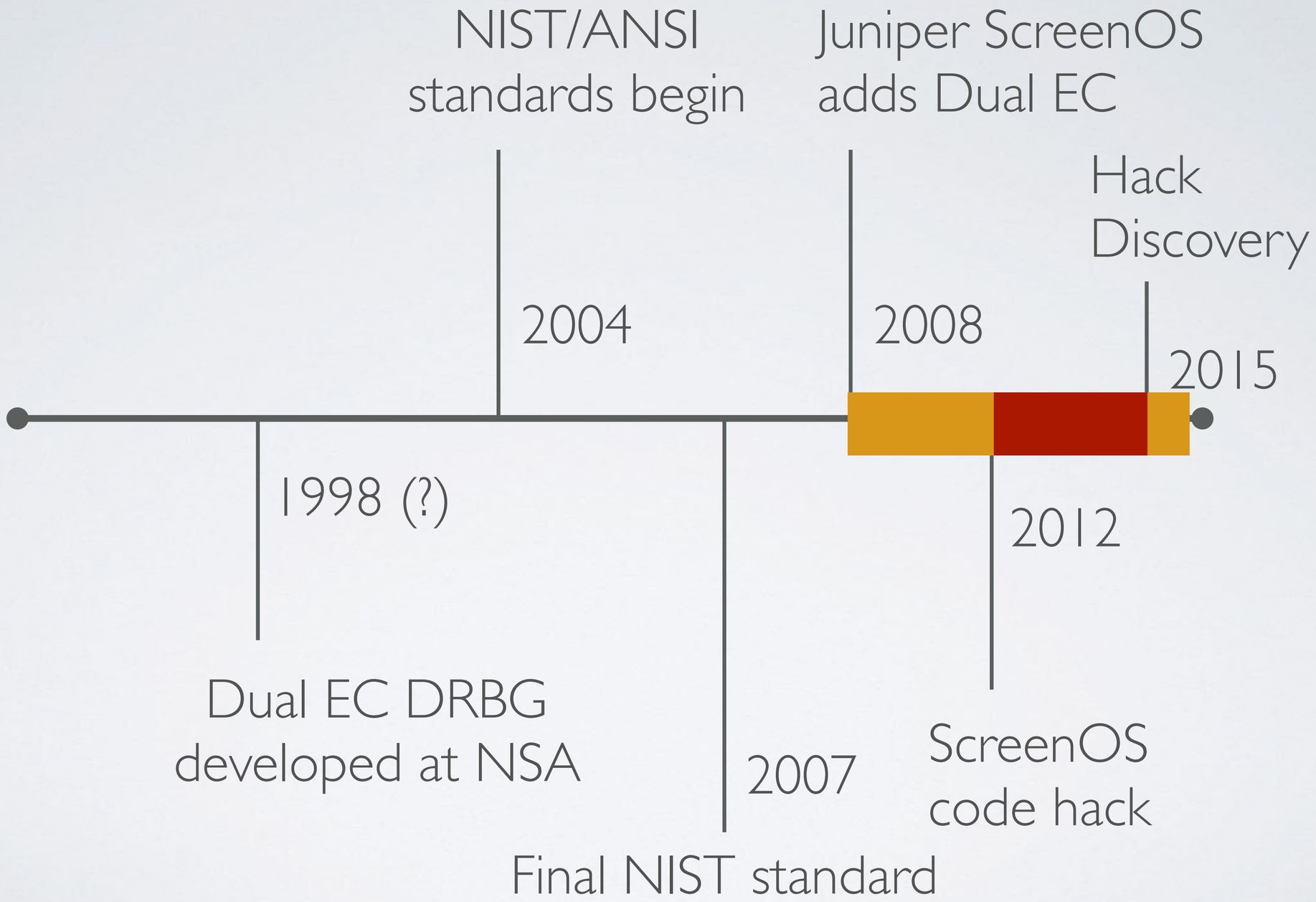
Credit: William Pinckaers

Revised Cascade



What does it all mean?

- **Juniper's code had an undocumented backdoor that could have been used (by the U.S. government) to spy on people**
- **Chinese (?) hackers broke into Juniper and re-purposed the U.S. backdoor and made it into their own**
- **Nobody found out for nearly two years**

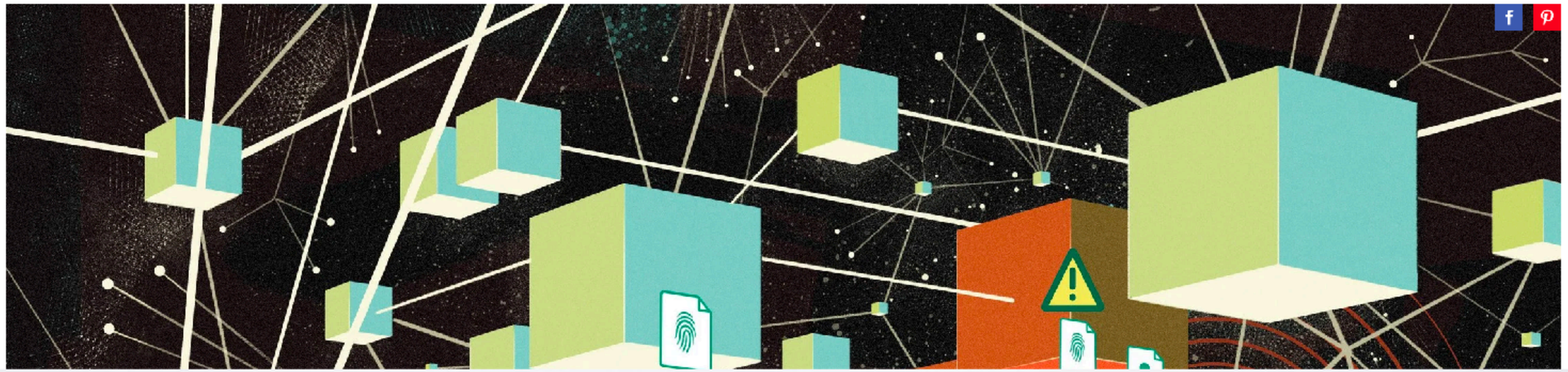

NIST/ANSI
standards begin
Juniper ScreenOS
adds Dual EC
Hack
Discovery
2004
2008
2015
1998 (?)
2012
Dual EC DRBG
developed at NSA
2007
ScreenOS
code hack
Final NIST standard

Who was the target?

Who was the target?

BRENDAN I. KOERNER SECURITY 10.23.16 5:00 PM

Inside the Cyberattack That Shocked the US Government



Who was the target?

OPM/OTM/NM/FIS Juniper Netscreen Support Consolidation - Bill of Materials FY13								
Support Coverage	Product	Serial#	Start Date	End Date	State	Zip Code	Unit Cost	Extended Cost
SVC-ND-ISG2000	NS-ISG-2000-SK1	0079062005000001	03-Feb-2014	02-Feb-2015	DC	20415		
SVC-ND-ISG2000	NS-ISG-2000	0079072009000003	03-Feb-2014	02-Feb-2015	DC	20415		
SVC-ND-ISG2000	NS-ISG-2000	0079082007000018	03-Feb-2014	02-Feb-2015	DC	20415		
SVC-ND-ISG2000	NS-ISG-2000	0079082007000393	03-Feb-2014	02-Feb-2015	DC	20415		
SVC-ND-ISG1000	NS-ISG-1000	0133032010000094	26-Jun-2013	02-Feb-2015	DC	20415		
SVC-EXT-WAR-ISG1000	NS-ISG-1000	0133032010000094	26-Jun-2012	25-Jun-2013	DC	20415		
SVC-ND-ISG1000	NS-ISG-1000	0133042010000041	26-Jun-2013	02-Feb-2015	DC	20415		
SVC-EXT-WAR-ISG1000	NS-ISG-1000	0133042010000041	26-Jun-2012	25-Jun-2013	DC	20415		
SVC-ND-ISG1000	NS-ISG-1000-SK1	0133042010000048	26-Jun-2013	02-Feb-2015	DC	20415		
SVC-EXT-WAR-ISG1000	NS-ISG-1000-SK1	0133042010000048	26-Jun-2012	25-Jun-2013	DC	20415		
SVC-ND-SSG140	SSG-140-SH	0185012008000001	26-Jun-2013	02-Feb-2015	DC	20415		
SVC-EXT-WAR-SSG140	SSG-140-SH	0185012008000001	26-Jun-2012	25-Jun-2013	DC	20415		
SVC-ND-SSG140	SSG-140-SH	0185012008000129	26-Jun-2013	02-Feb-2015	DC	20415		
SVC-EXT-WAR-SSG140	SSG-140-SH	0185012008000129	26-Jun-2012	25-Jun-2013	DC	20415		
SVC-ND-SSG140	SSG-140-SH	0185022008001383	26-Jun-2013	02-Feb-2015	DC	20415		

Ok, how might this have been exploited?

- **If the attacker is not a U.S. agency, this would require some means to gain network perspective**
  - (Passive access to network traffic)
  - This is relatively hard to do for non-US agencies
  - Idea: look for incidents of network traffic re-routing in the 2012-2015 period

One final note

- **In 2013, researchers noted the first durable BGP "MITM" interception events**
  - These are BGP events in which traffic is misdirected via one path, and reaches its destination via a different return path
  - These events were not detected before 2013, and have never been explained by any concrete software flaws
  - These deserve some more scrutiny

Going Dark

The EARN IT Act Is a Sneak Attack on Encryption

The crypto wars are back in full swing.


I WANT TO
BELIEVE