Chicken Coops, A Blackbird & the NSA

Scott Bradner

ABCD @400

2019-02-01

1

Double dose

- If you have nothing else to do

FEB 5, 2019 @ 12:00 PM

A History of the Internet

FEATURING SCOTT BRADNER

Please join us for The History of the Internet featuring Scott Bradner who worked in the areas of computer programming, system management, networking, IT security and... MORE ›

RSVP REQUIRED

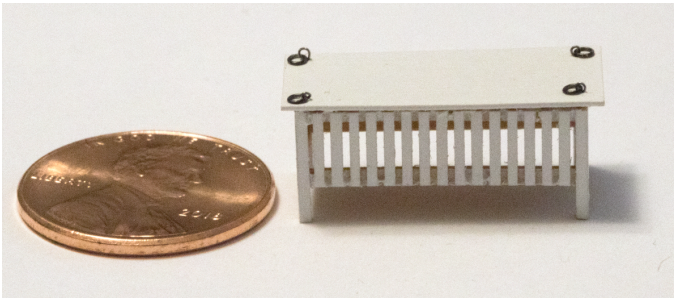
https://cyber.harvard.edu/events

2

The Model

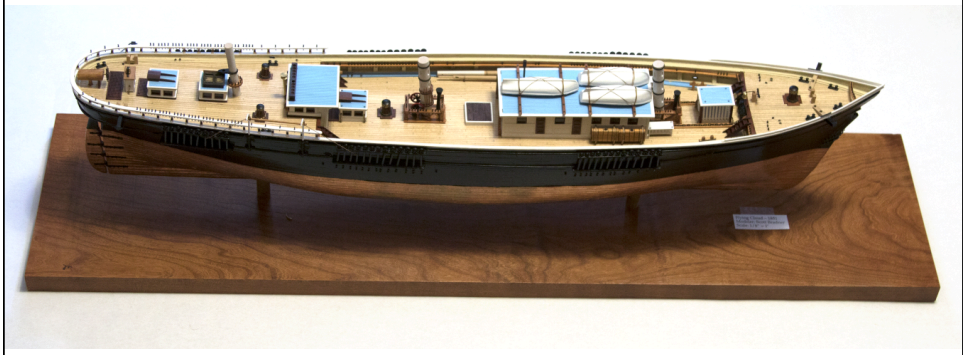
- It's done

  At least as much as it will ever be
- Bad kit distorted some basic features so starting again
- Last detail added – chicken coops



3

As-Is



4

Model at Model Show

5

YART

- Yet Another Road Trip
- Stats:

  May 20 – June 25

  8,580 miles

  22.2 MPG average

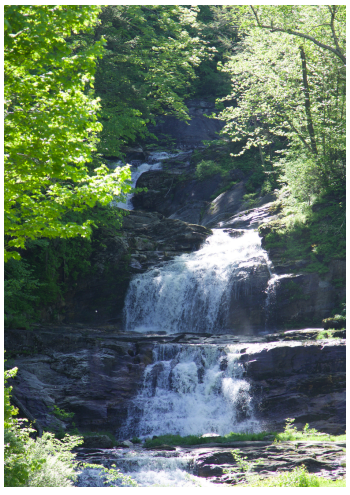
  zero speeding tickets ☺

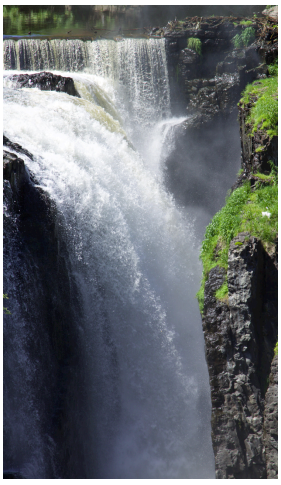
6

Path

7

Falling Water



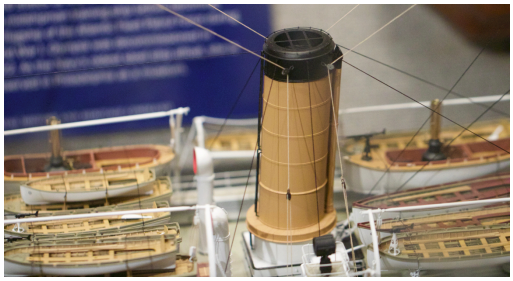


8

Not Falling Water

9

Power (Old-ish)



10

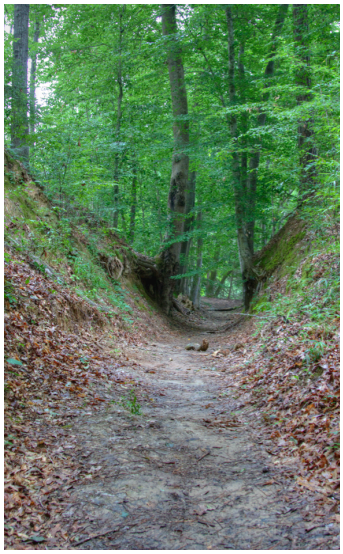
Power (Older)

11

Contrast

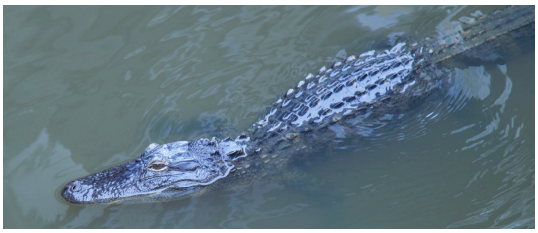
12

Natchez Trace (again)



13

Local Color



14

They Do Know How To Do Trees

15

Patterns 1

16

Patterns 2

17

Art

18

Lighter Than Air?

19

From When I Started

20

Blackbird!

21

Joy

22

Wikimedia v. NSA

Case: https://en.wikipedia.org/wiki/Wikimedia_Foundation_v._NSA
Report: https://www.sobco.com/declarations/Wikimedia-2018-12-18.pdf

23

Questions

- Actual:

  Is the NSA violating the 4th Amendment to the U.S. Constitution in the Upstream Collection program?

- But first:

  Does Wikimedia have "standing" to ask a court to answer the actual question?

24

4th Amendment

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

25

Standing

- To bring lawsuit an entity (e.g. a person or organization) must have "standing"
- Standing requires showing
  1/ that a legal wrong took place
    "legal wrong" is an action prohibited by law
  2/ a personal stake
    the wrong was against the entity
- I was asked to explore #2

26

My Tasks

a. What is the basic structure of the Internet and how do communications traverse it?
b. How does upstream collection work, based on official government acknowledgments and my expertise in network design and operation?
c. What is the likelihood that the government has copied and reviewed the plaintiff's international text-based Internet communications in the course of upstream collection?

27

Internet: History

- Started with ARPA which was a reaction to Sputnik
- ARPANET interconnected computers at research institutions starting in 1969
- Upgraded in 1983 to interconnect networks "the Internet"
- International connections by 1980
- Commercial Internet service providers (ISPs) took over by 1995
- ISPs interconnect at will − no fixed architecture

28

Internet: Communications

- Communications broken into packets
- Packets routed independently through networks
- Sets of packets reassembled into communications at receiving end
- Communications managed by applications in end systems

  email (SMTP, IMAP), world wide web (HTTP/HTTPS), telephone (SIP)

  network

29

Internet: International Connections

- Some terrestrial (Canada & Mexico) most undersea - all these are fiber

30

NSA Collection Programs

- The NSA collects copies of communications involving non-U.S. persons under the authority of Section 702 of the Foreign Intelligence Surveillance Act, as amended.
- Two collection programs
  - PRISM
  - upstream collection
- Targeting procedures approved by FISA court
- Both programs use *selectors* to identify target's communications that are to be collected
  - "collected" means ingested into NSA databases

31

Selectors

- *a unique identifier associated with the target - for example, a telephone number or an email address. This unique identifier is referred to as a selector. The selector is not a "keyword" or particular term (e.g., "nuclear" or "bomb"), but must be a specific communications identifier (e.g., e-mail address)*
- Selectors are *electronic communication accounts/ addresses/identifiers*
- IP addresses may not be good selectors because they often do not uniquely identify an individual and they can change often

32

PRISM Collection

In PRISM collection, the government sends a selector, such as an email address, to a United States-based electronic communications service provider, such as an Internet service provider ("ISP"), and the provider is compelled to give the communications sent to or from that selector to the government

- This case does not concern PRISM collection

33

Upstream Collection

Once tasked, selectors used for the acquisition of upstream Internet transactions are sent to a United States electronic communication service provider to acquire communications that are transiting through circuits that are used to facilitate Internet communications, what is referred to as the "Internet backbone." The provider is compelled to assist the government in acquiring communications across these circuits. To identify and acquire Internet transactions associated with the Section 702–tasked selectors on the Internet backbone, . . .

34

Upstream Collection, contd.

. . . Internet transactions are first filtered to eliminate potential domestic transactions, and then are screened to capture only transactions containing a tasked selector. Unless transactions pass both these screens, they are not ingested into government databases. As of 2011, the NSA acquired approximately 26.5 million Internet transactions a year as a result of upstream collection

35

Target Communications

- Must not be "wholly domestic"

  I.e, at least one end outside the U.S.

  NSA is required to use other technical means, such as Internet protocol ("IP") filters, to help ensure that at least one end of an acquired Internet transaction is located outside the United States.

- Large filter − e.g., one list of U.S. IPv4 address prefixes contains 66 K entries

  Also, list can be quite dynamic with current market-based IP address assignment process

36

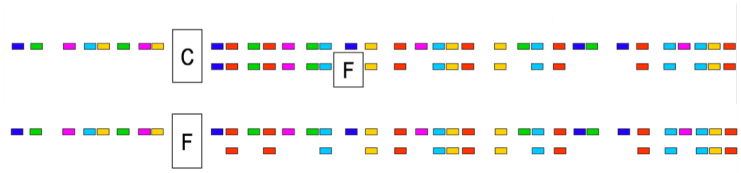
How Does It Work?

- The NSA has not disclosed all the details
- But there are not many options
- Basic steps gleaned from public NSA information
  a) Ignore communications on a communications link that are not from or to a non-U.S. network node
  b) Check to see if any remaining communications include an approved selector
  c) If a selector is present, import the communication into an NSA database
- Steps could be done directly by the NSA or by someone else under NSA direction

37

Ignore Non-U.S. Communications

- Communications consist of packets
- A filter that discards packets if both source and destination IP addresses in a packet are U.S. addresses would generally do this
- But, where does the filter sit?



- Note: either all packets are copied or all non wholly domestic packets are copied

38

Filter Out All-U.S. Communications

- The NSA says it does not always use a filter

  in those cases where NSA seeks to acquire communications about the target that are not to or from the target, NSA will either employ an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas, or [redacted] In either event, NSA will direct surveillance at a party to the communication reasonably believed to be outside the United States

39

Hint

the government readily concedes that NSA will acquire a wholly domestic 'about' communication if the transaction containing the communication is routed through an international Internet link being monitored by the NSA or is routed through a foreign server.

40

Check For Selectors

- Need to reassemble packet streams into the communications in order to be able to scan the communication for a selector since selectors could span packets
  - Conceivable to maintain enough state between packets to avoid reassembly but far easier to just reassemble the communications
- Also, if a communication contains a selector the NSA will need the reassembled communication to import into its databases
- Thus, very likely that all non-all-U.S. communications are reassembled

41

Summary #1

- It is highly likely that the NSA is copying all packets on links it is monitoring or, at least, all packets that include a non-U.S. source or destination address
- It is highly likely that the NSA is reassembling at least all communications that are from or are to non-U.S. locations
- The NSA must be reviewing the contents of the reassembled communications in order to see if they contain selectors

42

OK, But Where?

- Where would the NSA be doing its monitoring?
- Under the upstream collections program the NSA cannot collect wholly domestic communications
  The NSA can collect communications not from or to the U.S. under other programs
- Logically, the NSA should be monitoring at least the U.S. end of international communications links
- But which links?

43

International Links

- Many international fiber cables
- Each cable has multiple fibers
- Each fiber can support multiple channels
- Each channel acts as a communications link
- Some channels are used for internal corporate communications, others are used between or within ISPs
- Thus there are many channels that could be carrying communications the NSA can collect under the upstream collections program

44

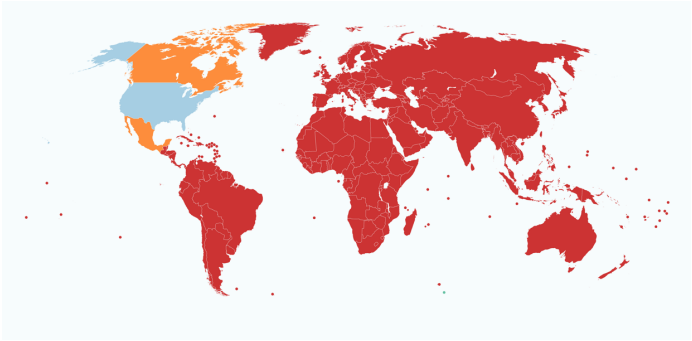
Which channels to monitor?

- The NSA has acknowledged that it has 129,000 Section 702 targets, all located outside the U.S.
- Communications between these targets and the U.S. will be directed by the Internet routing system via the "shortest paths"
- With such a large number of targets distributed around the world their communications will use most if not all the international channels that carry public Internet traffic

45

What About Wikimedia?

- Wikimedia includes 12 free-knowledge sites (e.g., Wikipedia, Wiktionary, Wikinews, Wikibooks, Wikisource)
- Users in all of the world's inhabited continents and islands − 380 billion requests 8/1/17 to 1/31/18



46

Wikimedia Communications

- With such a wide distribution of users, Wikimedia traffic is using all international channels that carry public Internet traffic
- i.e., Wikimedia traffic is using all of the international channels the NSA is monitoring

47

Conclusion

- Since the NSA must be copying, reassembling and reviewing at least all non-all-U.S. communications on the links it is monitoring, it must be the case that the NSA has copied, reassembled and reviewed at least some Wikimedia communications

48

Thank You for listening

Questions?

49