Feds and 0Days:
From Before Heartbleed to After FBI-Apple

@Jason_Healey

Columbia University

SIPA

Today's Talk

1. How does US government decide to retain or disclose 0days vulnerabilities?
2. How many 0days does the US government keep to itself every year?
   – Hundreds? Thousands? More? Less?
3. How big is the full US arsenal of 0days?
   – Hundreds? Thousands? More? Less?
4. What we don't know & recommendations

About the Research Team

- Reports due by early fall of 2016
- Students and professor from SIPA
  - Columbia University's School of International and Public Affairs
- One foot in each community: DC and policy

SIPA

Student Research Teams

- **Team 1**: Jackie Burns-Koven, Natasha Cohen, and Andrew Liu
  - 0day markets and government involvement
- **Team 2**: Mellissa Zubaida Ahmed, Igor Bakharev, Robert Diamond, Nozomi Mizutani, Jittip Mongkolnachaiarunya, Nicole Softness
  - US government vulnerability disclosure program
- **Team** 3: Arsla Jawaid, Laurence Kinsella, Andrew Pfender, Arastoo Taslim
  - Security researchers and corporate vulnerability programs, such as responsible disclosure and bug bounty programs
- **Team 4**: Niko Efstathiou, Daniel Ismael Gonzalez, Marie von Hafften, Adriana Tache
  - Vulnerability databases and quant measurement
- **Team 5**: Sherman Chu, Timothy Hodge, Caitlin LaCroix, Amine Moussaoui, Anthony Sanford
  - Actual use of 0days in the wild and whether other nations have explicit 0day policies

SIPA

2008

A working group was established and developed the Joint Plan to improve the government's ability to use the full spectrum of offensive capabilities to better defend U.S. information systems. One recommendation within the Plan was the development of a VEP.

Drafters of the 2010 VEP: A follow-on working group led by the ODNI was established to address the recommendation with representatives from the Intelligence Community (NSA, CIA, DIA, ODNI), Attorney General, FBI, DoD, DoS, DoE, and DHS. The end result of the working group is a community-wide coordinated document titled, "Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process", officially describing the details of VEP.

2009

2010

According to the government's revelation in 2014, **VEP Policy went in effect in this year.** In the year, Stuxnet, the program employed by the U.S. and Israel to cripple much of Iran's uranium enrichment project by using four different zero day vulnerabilities, was also found.

2011

2012

2013

It is reported that the NSA allocated $25.1 million to purchasing vulnerabilities during fiscal year 2013.

December: In a wake of Snowden's revelation, the **President's Review Group on Intelligence and Communications Technologies** was created to provide recommendations for reforming the intelligence community's activities. Some of the recommendations include:

- Disclosing vulnerabilities by default
- Shift in the "equities" process from the NSA to the White House. This implies that until this year the NSA or the intelligence community had been the sole arbiter of decisions about the use of zero-day vulnerabilities and exploits.

2014

March: Vice Admiral Michael Rogers' testimony during the confirmation hearing to replace Gen. Keith Alexander as head of the NSA and the U.S. CYBERCOM was the **first public description of NSA zero-day policy**, hinting that the government's policy in this area was beginning to **lean more toward disclosure than exploitation**. He also mentioned about interagency process working with White House.

14 April: Two days after a news report falsely claimed the NSA had known about the Heartbleed and kept silent to exploit it, ODNI **finally went public with a formal statement about its VEP policy** and denied the claim. In response to the Review Group's

2014

28 April: Vice Admiral Michael Rogers' testimony during the confirmation hearing to replace Gen. Keith Alexander as head of the NSA and the U.S. CYBERCOM was the **first public description of NSA zero-day policy**, hinting that the government's policy in this area was beginning to **lean more toward disclosure than exploitation**. He also mentioned about interagency process working with White House.

6 May and 1 Jul: EFF filed a FOIA request for records related to these processes on 6 May, then filed suit against ODNI and NSA on 1 July to force disclosure of relevant documents, accusing them of violating the FOIA for failure to expedite processing and violating of the FOIA for wrongful withholding of agency records.

3 November: The CYBERCOM's new commander and the NSA's new director Admiral Rogers said at Stanford University that "by orders of magnitude, the greatest numbers of vulnerabilities we find, we share."

17 November: during Michael Daniel's interview with Wired, he stated that **he chairs an interagency group** at the White House, which then makes a final decision based on the recommendations from subject-matter experts. He also reiterated that the government's default position would be to disclose but that there "are a limited set of vulnerabilities that we may need to retain for a period of time in order to conduct legitimate national security intelligence and law enforcement missions."

2015

3 September: Although ODNI and NSA had gradually released the process-related documents since 15 December 2014 in response to the EFF's lawsuit, it was 3 September 2015 that it **released the official VEP document** entitled "Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process". However, the document was hugely redacted and referred to the VEP process as it existed under NSA's control as executive secretariat.

2016

January: Additional sections of the VEP document are released. The document is the first official acknowledgment of "defensive, offensive and/or law enforcement-related [and] prosecutorial" uses of the vulnerabilities beyond counterterrorism efforts.

March: A federal court in San Francisco upheld the few remaining redactions. Thus the VEP document released in January is regarded as the final version that the EFF (and the public) can get.

April: The FBI announces that it will not be submitting the exploit tool it purchased for an iPhone through the VEP.

Conviction and Research

- Levels of confidence
- Lines of evidence
- Suspicion
- Credibility
  - DC audience
  - Policy audience

- Will you be convinced?

Way Overly Simplified Basics of USG Role

Strong Tension, Often Bureaucratic Fighting Between Two Groups

- Three main users of vulns
  - DoD: warfare and espionage
  - Intelligence Community (esp NSA and CIA): espionage and covert action
  - Law enforcement: Justice, FBI, DHS
- Several whose "equities" want them closed
  - Commerce - running a vuln disclosure dialog
  - Treasury, Energy, et al
  - DHS (CIP and cyber)

Three Kinds of Online Targets Sets in Military Terms

Each With Different Vuln Issues

1. Closed battlefield
2. Closed and proprietary, more commercial or industrial
3. Open Internet, consumer focused

SIPA

Prehistory of USG Use of 0days

- USG used (and shared) vulns at least since 1990s
- US Air Force informal policy to retain vulns for offense use
  - Bejtlich: "We actually had a standing order after that that said, if you find something, you don't tell the vendor, you tell the offensive side, and they'll decide what to do about it.“ [FN1]
- Hoarded within military services, intelligence agencies
- Mid-1990s: NSA “Information Operations Technology Center”
  - Develop a common ‘toolbox’ of ‘capabilities’ based in part on vulnerabilities

Prehistory of USG Use of 0days

- White House gets involved with NSPD-16 in July 2002: “To Develop Guidelines for Offensive Cyber-Warfare”
  - Asserted presidential authority to coordinate capabilities and operations
  - Classified but doesn’t seem to specifically include policy on vulns

Prior to 2010, no formal US government-wide policy or process for handling vulns

SIPA

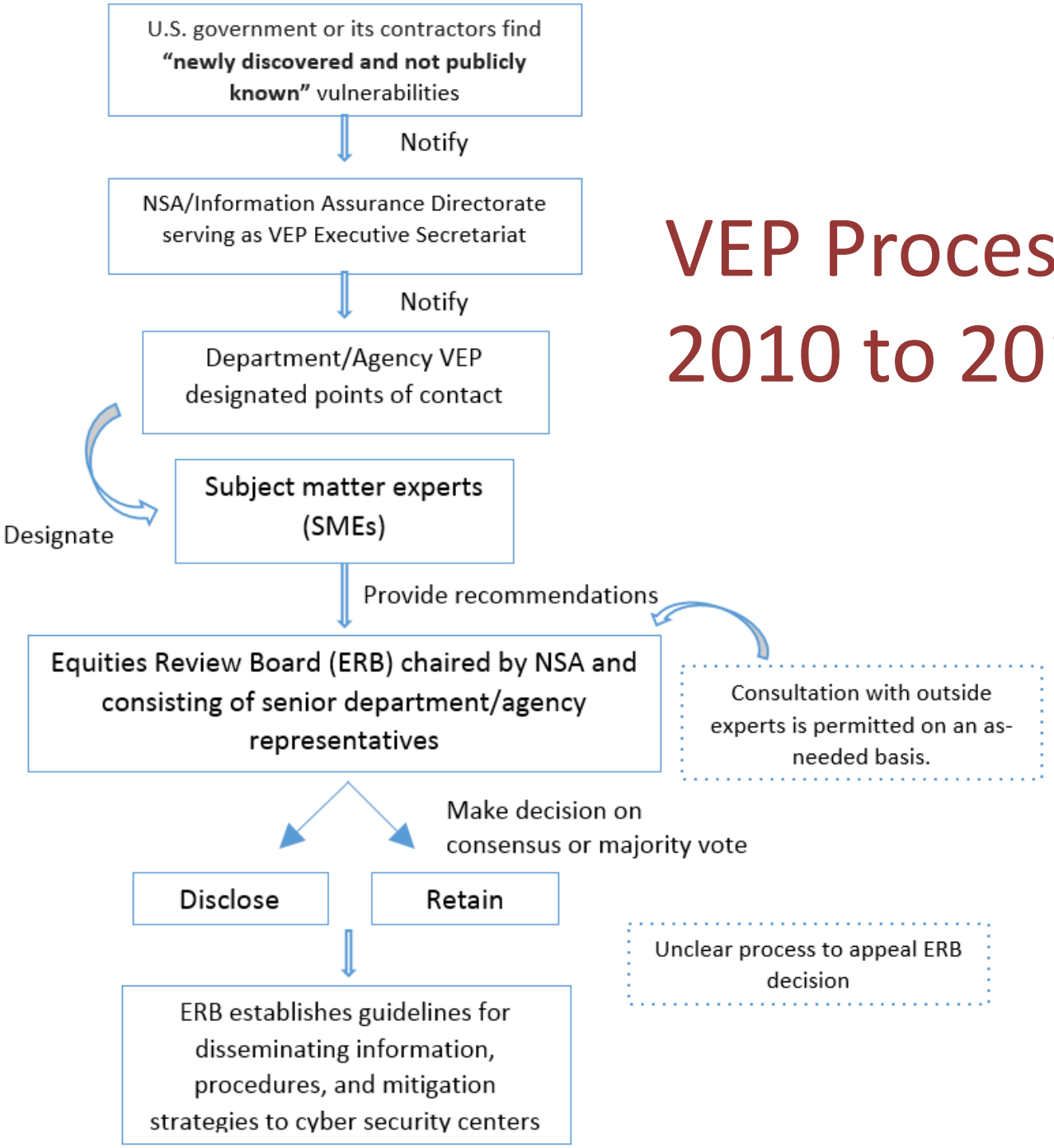
Pre-2010 USG 0-Day Policy

- NSA develops strong internal process based on 'intel gain/loss' and 'equities' decisions
  - Will US national interest be more served by sharing with vendors or keeping for our own use?
  - More likely to keep if NOBUS – so obscure or complex it is “not usable by anyone but us”
- Decision entirely up to DIRNSA
- Assume CIA, Justice had similar internal process

US Government Vulnerability Equities Process

- Formal new process in 2010 - we now know thanks to EFF [FN2]
  - Included 'interagency' review by other interested parties, including the defensive agencies
  - ODNI VEP document sets out
    - Process for notification, decision-making, and appeals
    - Established NSA as the Executive Secretariat

VEP Process 2010 to 2014



Policy from 2010 Not Fully Implemented

- “VEP was dormant. NSA continued to run their own internal process but did not formally include outside agencies.” [FN3]
- White House: Previous “default disclosure policy … not implemented to full degree” so needed to be “reinvigorated” [FN4]
  - Possibly driven by news of Stuxnet’s five 0days…

More Recent Fed 0day Process

- Post-Snowden review group recommends Obama strengthen process [FN5]
- Obama accepts recommendations deciding
  - Policy is to *disclose by default*
  - Centralize *decision power in the White House* rather than at NSA
- New policy enacted in January 2014 [FN6]

Congressional Testimony by Admiral Rogers
March of 2014 [FN7]

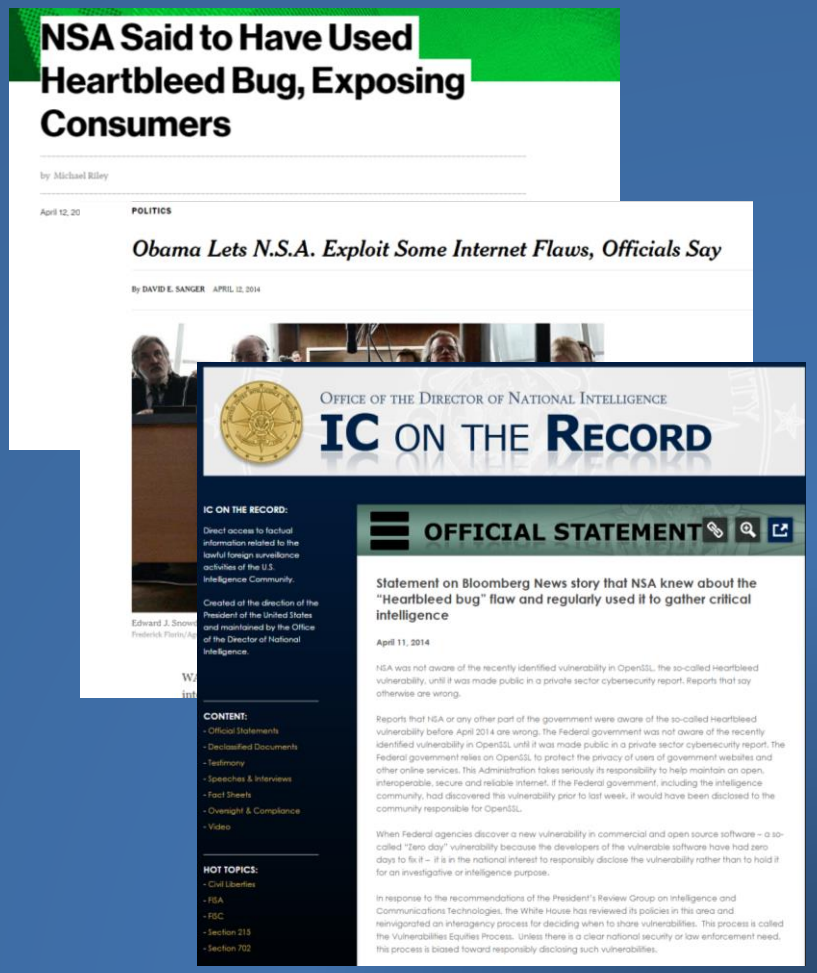
- "The *default is to disclose* vulnerabilities in products and systems used by the U.S. and its allies
- "*NSA has always employed this principle* in the adjudication of vulnerability findings
- "Within NSA, there is a *mature and efficient equities resolution process* for handling '0-day' vulnerabilities discovered in any commercial product or system (*not just software*) utilized by the U.S. and its allies
- "Technical experts document the vulnerability in full classified detail, options to mitigate the vulnerability, and a proposal for how to disclose it.
- "When NSA decides to withhold a vulnerability for purposes of foreign intelligence … [we] will *attempt to find other ways to mitigate the risks* to national security systems and other US systems"

More Recent Fed 0day Process

- Repeat: *White House policy is to disclose to vendors, not to keep for intel or warfighting*
  - Policy decision by the President himself and enforced by the National Security Council staff
  - About as strong as you can get in the Beltway
- But … Obama's decision carved out exceptions for national security or law enforcement
  - Three breakthroughs loomed, giving far more info

Breakthrough #1: Heartbleed Forces White House's Hand

- April 2014 Bloomberg story falsely trumpets that NSA knew about Heartbleed and kept for offense [FN8]
- Follow-up NYT story gets NSA to publicly deny they knew [FN9, FN10]

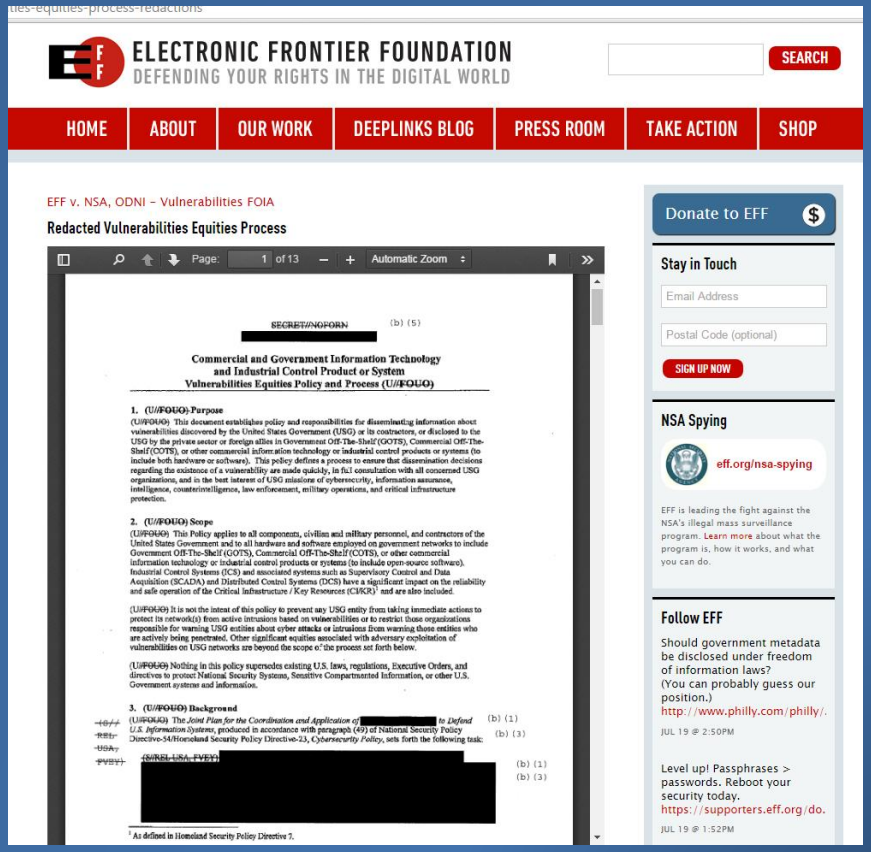


Heartbleed Forces White House's Hand

- 17 days after first, Bloomberg story…
- Extensive blog by NSC cyber coordinator Michael Daniel [FN11] outlines White House decision criteria on when to retain/disclose vulns:
  1. How much is the vulnerable system used in the core internet infrastructure, in other critical infrastructure systems, in the U.S. economy, and/or in national security systems?
  2. Does the vulnerability, if left unpatched, impose significant risk?
  3. How much harm could an adversary nation or criminal group do with knowledge of this vulnerability?
  4. How likely is it that we would know if someone else was exploiting it?
  5. How badly do we need the intelligence we think we can get from exploiting the vulnerability? Are there other ways we can get it?
  6. Could we utilize the vulnerability for a short period of time before we disclose it?
  7. How likely is it that someone else will discover the vulnerability?
  8. Can the vulnerability be patched or otherwise mitigated?

Breakthrough #2
EFF FOIA of Core VEP Documents

- In January 2016, EFF released documents pursuant to FOIA request and lawsuit [FN2]



Breakthrough #3



THE NATIONAL SECURITY AGENCY

Discovering IT Problems. Developing Solutions. Sharing Expertise

Q: When the U.S. Government learns of vulnerabilities in information-technology products, will it disclose information about those vulnerabilities?

A: **The U.S. Government takes seriously its commitment to an open and interoperable, secure, and reliable Internet. In the vast majority of cases, responsibly disclosing a newly discovered vulnerability is clearly in the national interest. We all rely on the Internet and connected systems for much of our daily lives. Plus, our economy would not function without them. For these reasons, disclosing vulnerabilities usually makes sense. But there are legitimate pros and cons to the decision to disclose vulnerabilities, and the trade-offs between prompt disclosure and withholding knowledge of some vulnerabilities for a limited time can have significant consequences.**

The National Security Council has an interagency process to consider when to disclose vulnerabilities. The process requires the government to weigh many factors, including the importance of the information to the nation's security. While these decisions can be complex, **THE GOVERNMENT'S BIAS IS TO RESPONSIBLY AND DISCREETLY DISCLOSE VULNERABILITIES.**

For many years prior to the establishment of the interagency process, NSA had an internal review process in this area. NSA's review continues and now informs the interagency process. Historically, NSA has released more than

91 **PERCENT OF VULNERABILITIES DISCOVERED IN PRODUCTS THAT HAVE GONE THROUGH OUR INTERNAL REVIEW PROCESS AND THAT ARE MADE OR USED IN THE UNITED STATES.**

The remaining 9% were either fixed by vendors before we notified them or not disclosed for national security reasons.

DISCLOSING A VULNERABILITY CAN MEAN THAT WE FORGO AN OPPORTUNITY TO:

Collect crucial foreign intelligence that could thwart a terrorist attack.

Stop the theft of our nation's intellectual property.

Discover even more dangerous vulnerabilities that are being used to exploit our networks.

THE **MEN** AND **WOMEN** OF NSA **MAKE A DIFFERENCE.**

For more than 60 years, the National Security Agency has worked to ensure that appropriate security solutions are in place to protect our critical infrastructure, national security systems, and the information on those systems. NSA's Information Assurance Directorate pioneered what is now called cybersecurity. We make information and information technology an asset for the United States – and a liability for its adversaries.

Learn more at www.nsa.gov/ia

NSA Infographic, 30 October 2015 [FN12]

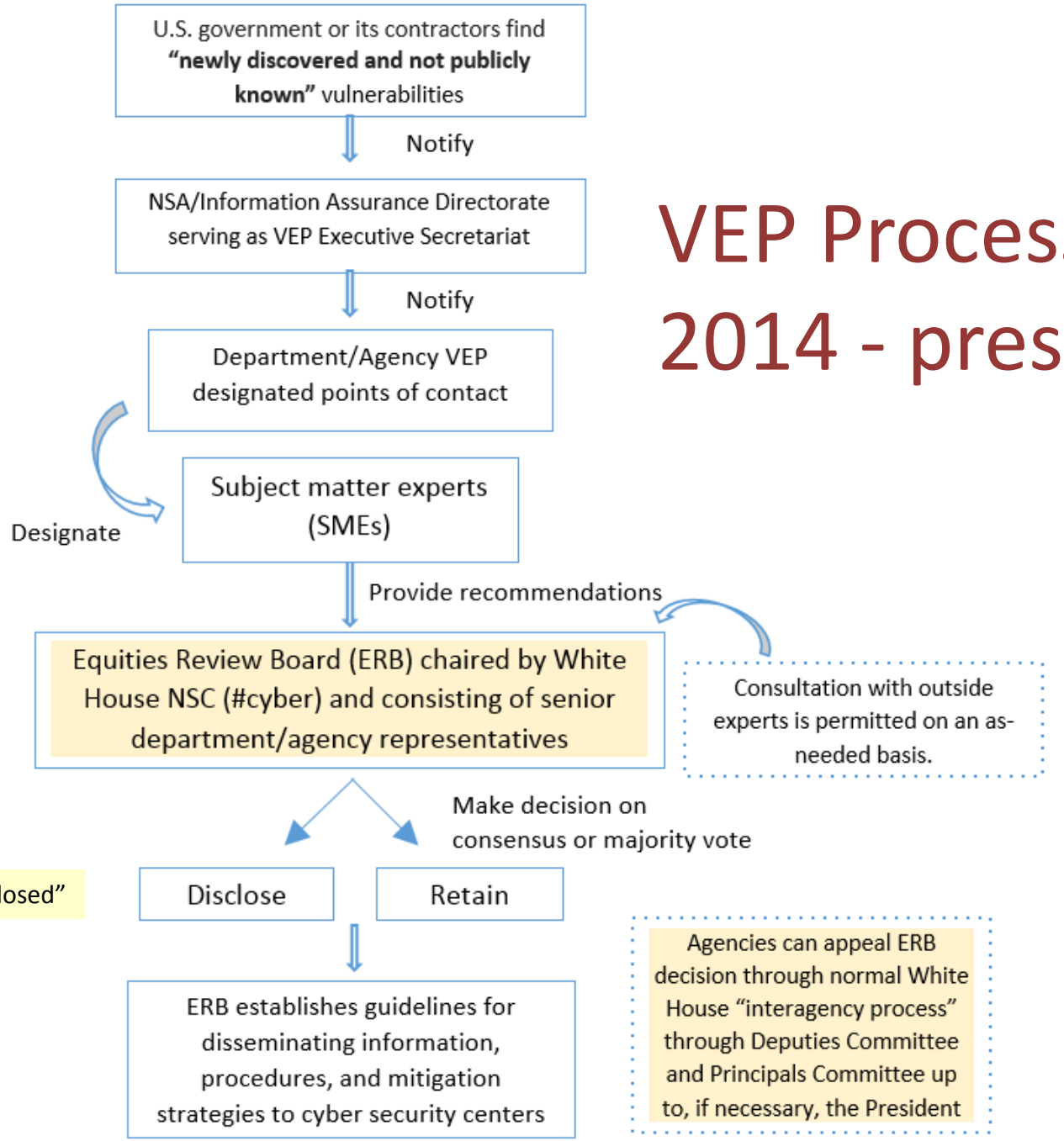
For many years prior to the establishment of the interagency process, NSA had an internal review process in this area. NSA's review continues and now informs the interagency process. Historically, NSA has released more than

91 **PERCENT OF VULNERABILITIES DISCOVERED IN PRODUCTS THAT HAVE GONE THROUGH OUR INTERNAL REVIEW PROCESS AND THAT ARE MADE OR USED IN THE UNITED STATES.**

The remaining 9% were either fixed by vendors before we notified them or not disclosed for national security reasons.

- Only NSA, not all USG
- Use of word "historically" implying this includes all NSA vulns back at least to 2020
- 9% not disclosed includes those already fixed by vendors

VEP Process 2014 - present



What We Learned from Breakthroughs

- Applies to all Feds and contractors and all vulns whether discovered or bought
- "Newly discovered and not publicly known"
  - Does not apply to vulns found *prior* to the policy
- New process not owned by NSA but by White House, which makes final decision
- Subtle inside-the-Beltway point:
  - Within White House, ERB run by Cyber Directorate, not intel or defense directorates

SIPA

What Don't We Know from Breakthroughs

- Making sense of Apple-FBI
- How many vulns does USG keep each year?
  - Hundreds, thousands, millions?
- Can we independently verify the USG claims?
- How large is existing USG 0day arsenal?
  - Hundreds, thousands, millions?
- Other nations' programs

SIPA

FBI v Apple (1)

- FBI should have had to submit iPhone 5 vuln to VEP
- Based on Daniel criteria, almost certainly would have had to disclose to Apple [FN13]
- FBI claiming contractual IP restrictions
  - Don't actually know what vulnerability and only bought the *use* of the tool [FN14]
  - So cannot possibly submit to VEP as don't know the vuln

SIPA

FBI v Apple (2)

- Seems to contradict pretty clear Presidential guidance, not sure yet if it is intentional
- Implications: yet to see if NSC will re-vamp the VEP guidance to specifically provide policy to close this loophole
- Side note: FBI informed Apple of a vuln for the first time under the VEP in April 2016 [FN15]

How Many Vulns Did USG Retain?

Prior to “Reinvigorated Policy”

How Many Vulns Did USG Retain?
Prior to "Reinvigorated Policy"

- Not hundreds or thousands per year but probably *dozens*
  - Moderate confidence in this assessment

How Many Vulns Did USG Retain?
Prior to "Reinvigorated Policy"

- Not hundreds or thousands per year but probably *dozens*
  - Moderate confidence in this assessment
  - NSA had 2013 budget of $25.1 million for "additional covert purchases of software vulnerabilities" [FN16]
  - Does not count any bought by other agencies or discovered internal to NSA
  - What can this tell us?
  - Assumptions:
    - No bucket of bugs
    - Some purchase of non-commercial vulns
    - Tend towards higher value vulns
    - "91%" is roughly accurate (more on this later)

Can We Believe 91%?

- Dickie George, former IAD:
  - Retaining was “very rare” [FN17]
- Former DIRNSA Hayden:
  - “consistent with my experience … NEVER taken lightly. Might have previously, trended toward offense … but always taken seriously and fulcrum [towards defense] shifted over time” [FN18]
- Only applies to NSA not all of government
- Need evidence from vendors, but out of scope
- Assume accurate-ish for now

How Many Vulns Did USG Retain?
Prior to "Reinvigorated Policy"

- Example 1:
  - Purchases
    - 250 x important commercial vulns @ $100k each
    - 250 total commercial vulns of which 91% disclosed
  - ~25 total of vulns purchased per year are retained
    - Assume similar number purchased from other agencies and similar number discovered
  - Total retained: ~75
    - Even with marging of error of 3x, still only ~225 retained

How Many Vulns Did USG Retain?
Prior to "Reinvigorated Policy"

- Example 1:
  - Purchases
    - 250 x important commercial vulns @ $100k each
    - 250 total commercial vulns of which 91% disclosed
  - ~25 total of vulns purchased per year are retained
    - Assume similar number purchased from other agencies and similar number discovered
  - Total retained: ~75
    - Even with marging of error of 3x, still only ~225 retained

- Example 2:
  - Purchases
    - 12 critical commercial vulns @ $1 million
    - 5 critical non-commercial vulns @ $1 million
    - 32 major vulns at $250k
    - 44 total commercial vulns of which 91% disclosed
  - ~5 total of vulns purchased per year are retained
    - Assume similar number purchased from other agencies and similar number discovered
  - **Total retained: ~15**
    - Even with margin of error of 3x, still only ~45

How Many Vulns Does USG Retain *Today*?

How Many Vulns Does USG Retain *Today*?

- Not hundreds or thousands per year but *single digits*
  - High confidence in this assessment

SIPA

How Many Vulns Does USG Retain *Today*?

- Not hundreds or thousands per year but *single digits*
  - High confidence in this assessment
  - Press reported that in one year (probably 2015) the USG kept "only about two for offensive purposes out of about 100 the White House reviewed" [FN19]
  - NSA executive responsible for disclosure for 15 years, Dickie George, confirmed “on average that three or four flaws were withheld a year” [FN17]
  - Was told by NSA TAO and IAD leadership in autumn of 2014 that *zero* so far retained that year

Can We Prove or Disprove This?
Lines of Evidence

- Method 1: Historical and other comparisons
  - Consistent information from multiple sources with no dissenting information



Can We Prove or Disprove This?
Lines of Evidence

- Method 1: Historical and other comparisons
  - Consistent information from multiple sources with no dissenting information
- Method 2: Compare to total known 0days
  - Between 40 (per Brian Martin) or 54 (per Symantec) 0days found in the wild in 2015
  - USG retention of single digits reasonable





Can We Prove or Disprove This?
Lines of Evidence

- Method 1: Historical and other comparisons
  - Consistent information from multiple sources with no dissenting information



- Method 2: Compare to total known 0days
  - Between 40 (per Brian Martin) or 54 (per Symantec) 0days found in the wild in 2015
  - USG retention of single digits reasonable



- Method 3: NVD/CVE for statistical evidence
  - Tried but data too messy

Probably impossible

Can We Prove or Disprove This?
Lines of Evidence

- Method 1: Historical and other comparisons
  - Consistent information from multiple sources with no dissenting information
- Method 2: Compare to total known 0days
  - Between 40 (per Brian Martin) or 54 (per Symantec) 0days found in the wild in 2015
  - USG retention of single digits reasonable
- Method 3: NVD/CVE for statistical evidence
  - Tried but data too messy
- Method 4: Look for conflicting evidence
  - Evidence from vendors receiving vulns
  - Political fall-out?





Probably impossible

Out of Scope



Can We Confirm Independently?
Lines of Evidence

- Method 5: Calculating from the total number of *all* USG discovered vulnerabilities
  - George revealed NSA disclosed ~1,500 vulns per year [FN17]
  - NSA's 91% disclosure rate of 1,500 yields 135 vulns
  - Does not fit "single digits" but George confirmed that retaining was "very rare"

Potentially supports "dozens" retained before "reinvigorated" process

How Large is USG 0day Arsenal?

How Large is USG 0day Arsenal?

- Probably dozens of vulns, not hundreds or thousands
  - Moderate confidence

How Large is USG 0day Arsenal?

- Probably dozens of vulns, not hundreds or thousands
  - Moderate confidence
  - Arsenal would be function of
    - How many years of retaining 0days: at least 15
    - Number of 0days retained per year: single digits
    - Average number burned per year: say 50% (?)
    - Average life of 0day once used: ~300 days [FN20]
    - Average discovered by vendors or used by other actors: 25%
    - Average half-life of a 0days if not used: 12 months (?)
  - Difficult to get total > 50 or 60
    - Likely too many either used by USG or other or simply become obselete
    - This count does not include 'battlefield' or other non-commercial systems
  -

"The idea that we have these vast stockpiles of vulnerabilities stored up—you know, Raider's of the Lost Ark style—is just not accurate."

How Large is USG 0day Arsenal?

- Probably dozens of vulns, not hundreds or thousands
  - Moderate confidence
  - Arsenal would be function of
    - How many years of retaining 0days: at least 15
    - Number of 0days retained per year: single digits
    - Average number burned per year: say 50% (?)
    - Average life of 0day once used: ~300 days [FN20]
    - Average discovered by vendors or used by other actors: 25%
    - Average half-life of a 0days if not used: 12 months (?)
  - Difficult to get total > 50 or 60
    - Likely too many either used by USG or other or simply become obselete
    - This count does not include 'battlefield' or other non-commercial systems
  - *NSA catalog of capabilities had 50 listed* [FN21]

"The idea that we have these vast stockpiles of vulnerabilities stored up—you know, Raider's of the Lost Ark style—is just not accurate."

SIPA

Other Nations

- ~30 nations have offensive programs
  - US, UK, Canada, Thailand, Sweden, Australia, China, Russia, Netherlands
- UK only other that speaks on the issue:
  - GCHQ announced disclosure of 20 vulns in 2016 (as of late April) [FN22]
- Love 'em or hate 'em, but United States Government only one with such transparency in process and overall numbers

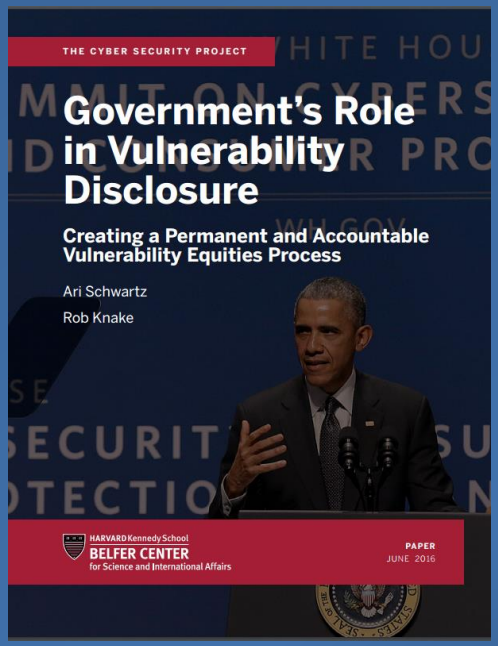
SIPA

Additional Research Questions

1. Are agencies really submitting *all* vulns to VEP?
2. Can agencies use vuln while it goes through VEP process? [FN23]
3. Is there a more direct measurement available of the arsenal?
4. How will the next president change the process?

Recommendations for Governments

- Former NSC officials Rob Knake and Ari Schwartz [FN24]
  - Formalize process as Executive Order or Presidential Directive
  - Periodic review of retained vulns
  - Transfer Executive Secretary function from NSA to DHS
  - Annual public report
  - Expand Congressional role
  - Mandate USG watchdog reporting: IGs and PCLOB
- Mandate *no use* until vuln through VEP
- More NSC direction to and accountability over executive secretariat
- Other democratic nations should have similarly transparent processes



SIPA

Recommendations for the Rest of Us

- Disclose to vendors to disarm governments
  - Only kind of conflict where one side can disarm the other by foregoing a new capability!
  - If you get rid of your nukes, your adversary still has their own. If you disclose a vuln, you take it away from all sides! (from Joe Nye)
- More attention from the community, academia, journalists
- More FOIA please!

SIPA

Today's Talk

1. How does US government decide to retain or disclose 0days vulnerabilities?
2. How many 0days does the US government keep to itself every year?
   – Hundreds? Thousands? More? Less?
3. How big is the full US arsenal of 0days?
   – Hundreds? Thousands? More? Less?
4. What we don't know & recommendations

SIPA

References

1. http://www.npr.org/2013/02/12/171737191/in-cyberwar-software-flaws-are-a-hot-commodity
2. https://www.eff.org/document/vulnerabilities-equities-process-redactions
3. Former WH official, email communication to Jason Healey, July 2016
4. https://www.wired.com/2014/11/michael-daniel-no-zero-day-stockpile/
5. https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf, recommendation #30
6. http://www.nytimes.com/2014/04/13/us/politics/obama-lets-nsa-exploit-some-internet-flaws-officials-say.html?_r=0
7. http://www.armed-services.senate.gov/imo/media/doc/Rogers_03-11-14.pdf
8. http://www.bloomberg.com/news/articles/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-consumers
9. https://icontherecord.tumblr.com/post/82416436703/statement-on-bloomberg-news-story-that-nsa-knew
10. http://www.nytimes.com/2014/04/13/us/politics/obama-lets-nsa-exploit-some-internet-flaws-officials-say.html?_r=0
11. https://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities
12. https://www.nsa.gov/news-features/news-stories/2015/discovering-solving-sharing-it-solutions.shtml
13. http://www.csmonitor.com/World/Passcode/2016/0325/Opinion-Why-the-FBI-will-eventually-reveal-its-iPhone-hack-to-Apple
14. http://www.macworld.com/article/3061934/security/fbi-wont-share-its-iphone-hack-with-apple-because-its-unfamiliar-with-the-code.html
15. http://www.macrumors.com/2016/04/26/apple-fbi-security-flaw-disclosure/
16. https://www.washingtonpost.com/blogs/the-switch/wp/2013/08/31/the-nsa-hacks-other-countries-by-buying-millions-of-dollars-worth-of-computer-vulnerabilities
17. http://www.sfchronicle.com/business/article/NSA-reveals-hundreds-of-bugs-a-year-says-former-7396429.php
18. Email from General Michael Hayden to Jason Healey, July 2016
19. http://www.bloomberg.com/news/articles/2016-03-23/thank-you-for-hacking-iphone-now-tell-apple-how-you-did-it
20. https://users.ece.cmu.edu/~tdumitra/public_documents/bilge12_zero_day.pdf
21. https://en.wikipedia.org/wiki/NSA_ANT_catalog
22. http://motherboard.vice.com/read/gchq-vulnerabilities-mozilla-apple
23. http://mobile.reuters.com/article/idUSKCN0SV2XQ20151107
24. http://belfercenter.ksg.harvard.edu/files/vulnerability-disclosure-web-final3.pdf

SIPA

THANK YOU

@JASON_HEALEY

This research was funded in part by Columbia University's Global Policy Initiative and the Carnegie Corporate of New York