Security Risks of Government Hacking

Riana Pfefferkorn I September 2018

The Center for
Internet and Society

Security Risks of Government Hacking

Riana Pfefferkorn[1]
September 2018

Abstract: As the use of encryption and other privacy-enhancing technologies has increased, government officials in the United States have sought ways to ensure law enforcement's capability to access communications and other data in plaintext. One of those methods is government hacking, also called "equipment interference." Government hacking allows investigators to exploit hardware and software vulnerabilities to gain remote access to target computers. Some experts believe regulated government hacking is preferable to proposals for mandatory "backdoors" for accessing encrypted data. However, the security risks of government hacking have not been thoroughly explored. Understanding those risks is necessary for technologists and policymakers assessing the desirability of government hacking as a responsible option for law enforcement to achieve its objectives.

Table of Contents

A. Introduction 2
B. Security Risks of Government Hacking 3
  1. Disincentive for Vulnerability Disclosure 3
  2. Cultivation of a Market for Surveillance Tools and 0-Days........ 5
  3. Attackers Co-opt Hacking Tools Over Which Governments Have Lost Control 7
  4. Attackers Learn of Vulnerabilities Through Government Use of Malware 10
  5. Government Incentives to Push for Less-Secure Software and Standards 11
  6. Government Malware Affects Innocent Users 13
C. Conclusion 15
Acknowledgements 16

[1] Riana Pfefferkorn is the Cryptography Fellow at Stanford Law School's Center for Internet and Society.

A. Introduction

United States government agents have been pushing for capabilities that would ensure investigators' access to plaintext despite increasing encryption use. Technologists have played a critical role in identifying the security risks that would be created by various proposals to mandate government access to encrypted data—so-called "backdoors." In response, many experts have embraced the idea of regulated government hacking, also known as "lawful hacking" and "equipment interference."

Government hacking involves allowing investigators to exploit vulnerabilities in software and hardware products to gain remote access to computers that store data investigators want, and to then remotely search, monitor user activity on, or even interfere with the operation of those machines. Some technologists and policymakers view regulated government hacking as a "middle ground" for achieving law enforcement objectives without resorting to backdoors that undermine security. However, while the risks of encryption backdoors are well understood, we've seen comparatively little discussion about the security risks inherent in government hacking. Illuminating those risks is necessary in assessing the desirability of government hacking as a responsible option for ensuring law enforcement access to plaintext.

In 2016 and 2017, Mozilla and the Stanford Center for Internet and Society hosted a series of discussions designed to identify and debate important policy issues related to the practice of government hacking. The third discussion, convened in February 2017, brought together leading technologists to examine underexplored security risks stemming from government hacking. The conversation raised a number of policy concerns that need more attention. Without this attention, embracing government hacking could expand computer security risks unnecessarily and unadvisedly.

This paper addresses six main ways that government hacking can raise broader computer security risks. These include:

- Creating a disincentive to disclose vulnerabilities that should be disclosed because other attackers might independently discover them;
- Cultivating a market for surveillance tools and 0-days;
- Risking that vulnerabilities exploited by the malware will be identified and used by other attackers, as a result of either
  - law enforcement's losing control of the hacking tools, or
  - discovery by outsiders of law enforcement's hacking activity;
- Creating an incentive to push for less-secure software and standards; and
- Risking that the malware will affect innocent users.

B. Security Risks of Government Hacking

1. Disincentive for Vulnerability Disclosure

Vulnerabilities are flaws that can enable attackers to access a system, obtain or destroy data, or otherwise misuse it. When the government learns about a vulnerability in a piece of software or hardware, it can either exploit that vulnerability for its own purposes or can disclose it to the relevant software or hardware maker. When the vendor learns of the vulnerability, it may issue a patch, thereby limiting or ending the government's ability to exploit the flaw. At the same time, by patching, the vendor is making its users safe from other governments, identity thieves, and criminals. Governments thus face a choice. Should they keep information about the vulnerability secret, and protect their own hacking capabilities? Or should they disclose the vulnerability so the provider can patch, and thereby protect its product's users, including from the disclosing government itself?

The United States government purportedly goes through a Vulnerabilities Equities Process (VEP) to help it determine whether or not to disclose vulnerabilities.[2] Not all vulnerabilities the government uses go through this process: the VEP spells out circumstances where the government may choose not to put a vulnerability through the VEP. And where the government contracts with outside hacking firms who retain control of the information, the VEP is irrelevant.[3] Ultimately, the process, when it is used, is a chance for certain federal government agencies to assess the computer security risk posed by having a particular vulnerability the government controls remain unpatched. Assessing this risk is not, however, obvious or easy. Instead, these decisions, and policy overall, are based on unknowns.

For example, what is the likelihood that the same vulnerability has been or will be found by other attackers? In principle, there's no reason why two entities can't look at the same code and find the same flaw. Some experts point to the co-incident discovery of Heartbleed as an example—Google researchers found the flaw in SSL/TLS just a few days before research group Codenomicon did. Yet technology experts differ on the question of whether vulnerability rediscovery is common or relatively rare. Bugcrowd, which manages major companies' bug bounty programs, reported that in 2015, 32% of vulnerabilities submitted for purchase were duplicates, and in 2016 over 36% were.[4] Another study, from Bruce Schneier and

[2] White House, Vulnerabilities Equities Policy and Process for the United States Government (Nov. 15, 2017), https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.

[3] Robert K. Knake, FBI to Apple: We Would Probably Disclose the iPhone Flaw if We Knew What It Was, Council on Foreign Relations (Mar. 29, 2016), https://www.cfr.org/blog/fbi-apple-we-would-probably-disclose-iphone-flaw-if-we-knew-what-it-was.

[4] Bugcrowd, The State of Bug Bounty (July 2015), available at https://cdn2.hubspot.net/hubfs/1549768/PDFs/state-of-bug-bounty-08-2015.compressed.pdf;

Trey Herr, found rediscovery rates of 14% to 17% for vulnerabilities in browser software and 22% for bugs in the Android mobile operating system.[5] After their conclusions were criticized as inaccurate, Schneier and Herr updated their paper, revising their rediscovery rates slightly upward and concluding that "rediscovery takes place more often than previously thought."[6] On the other hand, the RAND Corporation issued a report analyzing a different set of data and put the rediscovery rate at only about 5% per year.[7]

What is more, bugs discovered by the U.S. government may be in a class of their own. In 2017 when the group "Shadow Brokers" released a set of National Security Agency (NSA) Windows hacking tools it had acquired (an issue discussed below), the code included four vulnerabilities that had never been independently discovered, as well as a fifth that had been previously discovered because someone was using it "in the wild" (another issue discussed below).[8] Dave Aitel, a former security scientist with the NSA and CEO of a vulnerability research and penetration testing tool development company, claims that "in reality, the vulnerabilities used by the US government are almost never discovered or used by anyone else."[9] This is in part because exploitable vulnerabilities are rare and creating reliable exploits that circumvent modern security defenses is extremely difficult.[10] If Aitel is right, then the government's choice not to disclose a vulnerability poses far less of a risk than if there is a 1-in-3 chance of rediscovery as the Bugcrowd reports indicate.

Ultimately, experts do not precisely know the rediscovery rate for any specific vulnerability or class of vulnerabilities, and aren't going to know anytime soon.

Bugcrowd, The State of Bug Bounty (June 2016), available at https://pages.bugcrowd.com/hubfs/PDFs/state-of-bug-bounty-2016.pdf.

[5] Kim Zetter, "Malware Attacks Used by the U.S. Government Retain Potency for Many Years, New Evidence Indicates," The Intercept (Mar. 10, 2017), https://theintercept.com/2017/03/10/government-zero-days-7-years/.

[6] Trey Herr and Bruce Schneier, "What You See Is What You Get: Revisions to Our Paper on Estimating Vulnerability Rediscovery," Lawfare (July 27, 2017), https://lawfareblog.com/what-you-see-what-you-get-revisions-our-paper-estimating-vulnerability-rediscovery (discussing the changes made to the initial version); Trey Herr, Bruce Schneier, and Christopher Morris, *Taking Stock: Estimating Vulnerability Rediscovery* (July 2017), http://www.belfercenter.org/sites/default/files/files/publication/Vulnerability%20Rediscovery%20%28belfer-revision%29.pdf (updated version of paper).

[7] Lillian Ablon and Andy Bogart, Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits (March 2017), RAND Corporation, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1751/RAND_RR1751.pdf.

[8] Bruce Schneier, Zero-Day Vulnerabilities against Windows in the NSA Tools Released by the Shadow Brokers (July 28, 2017), https://www.schneier.com/blog/archives/2017/07/zero-day_vulner.html.

[9] Dave Aitel, Slow Down On Lawful Hacking Frameworks and Fixes, Lawfare (Aug. 4, 2016), https://www.lawfareblog.com/slow-down-lawful-hacking-frameworks-and-fixes.

[10] Dave Aitel and Matt Tait, Everything You Know About the Vulnerability Equities Process Is Wrong, Lawfare (Aug. 18, 2016), https://www.lawfareblog.com/everything-you-know-about-vulnerability-equities-process-wrong.

Despite that shortcoming, ultimately, if law enforcement is using a particular vulnerability in investigations, it will be inclined to keep it secret (that is, if courts do not force prosecutors to reveal information in discovery in criminal cases). There will be a strong law enforcement disincentive against disclosure in any VEP evaluation.

Against sophisticated adversaries of the kind encountered by intelligence (e.g. foreign militaries), useful exploits are more likely to be *sui generis* (e.g. flaws in a uranium enrichment plant). However, for agencies with a more general population of attack targets, such as federal and state/local law enforcement, more generic vulnerabilities that affect more people are useful. So, the more that law enforcement relies on government hacking, the greater the incentive to keep quiet widespread security flaws. This increases the risk that disclosure will not happen even, or especially, when it would result in a security patch for the general population.

2. Cultivation of a Market for Surveillance Tools and 0-Days

A related security risk is cultivation of the 0-day market. 0-day is a term for vulnerabilities or exploits that have not been disclosed to vendors. In other words, vendors have had zero days to fix the problem. When governments hack, sometimes they will seek to develop their own vulnerabilities. But sometimes they will purchase them, or purchase the right to use them, as the Federal Bureau of Investigation (FBI) did in 2016 with a tool that enabled it to unlock one of San Bernardino shooter Syed Riswan Farook's mobile phones. (The FBI reportedly paid hundreds of thousands of dollars, though this amount is ostensibly an outlier.[11])

Today we have companies that are in the business of developing and selling 0-days, with no intention of revealing the flaw to the vendor so that it may be fixed. 0-days are generally used by state actors, may not be very common, and are not the biggest security problem out there. The existence of a market for 0-days may incentivize the discovery of more vulnerabilities. Some think that could lead to better security overall, so long as the government buying the 0-day ultimately discloses it to the vendor to be fixed. But that assumes 0-days are relatively rare; if they are plentiful, then an active 0-day market could be harmful.[12]

Companies that sell 0-days are often questioned as to whether they do business with human rights-violating nations, organized crime, or other abusive actors. For example, NSO Group, a vendor of "lawful intercept" spyware products, sold malware

[11] Nathan Ingraham, "Senator Confirms FBI Paid $900,000 to Unlock San Bernardino iPhone," Engadget (May 8, 2017), https://www.engadget.com/2017/05/08/fbi-paid-900000-to-unlock-san-bernardino-iphone/.

[12] Bruce Schneier, "Should U.S. Hackers Fix Cybersecurity Holes or Exploit Them?", *The Atlantic* (May 19, 2014), https://www.theatlantic.com/technology/archive/2014/05/should-hackers-fix-cybersecurity-holes-or-exploit-them/371197/.

containing 0-days to governments that then used it to target devices belonging to journalists, scientists, human rights activists, politicians, and others.[13]

Responsible 0-day vendors put contractual mechanisms in place to prevent such abuse or reselling to such actors. Ultimately, however, these companies have little insight and less control over what happens once the 0-day is turned over. Vendors can't fully vet their clients or prospective use cases, which are sometimes classified. A company cannot generally audit a government to assess whether it misuses a 0-day. If it does, what is the company's recourse—suing the government for breach of contract? 0-day vendors have little incentive to reliably check government abuses. To the contrary, if abusive regimes are willing to pay more than non-abusive governments, 0-day vendors have an explicit incentive to look the other way.

The U.S. government may exacerbate these problems when it is an active customer of 0-day vendors. Its purchase of 0-days both incentivizes the development and sale of 0-days, and also gives the U.S. less moral credibility to object when unscrupulous 0-day vendors sell to oppressive nations. On the other hand, some argue that U.S. market power could be leveraged to punish vendors who sell to human rights abusers and other oppressive regimes. However, that may be unlikely under the current administration, which does not have a consistent track record of strongly opposing such abuses and the regimes that commit them. And still others question the U.S.'s market power in the 0-day space. They argue that the 0-day market will evolve with or without U.S. participation, and that there will be other major players, be they democratic nations or less-reputable actors, making that market robust.

Whatever the impact of U.S. participation in the 0-day market, letting 0-day vendors have too much say over the government's use of a 0-day can *also* pose a security risk. 0-day vendors are not in the best position to decide what security vulnerabilities the affected product's developer should or shouldn't know about. Yet the FBI did not disclose to Apple how it unlocked Farook's iPhone, claiming that the company that provided the tool, and not the FBI, owned the vulnerability, so it was not subject to the VEP. The FBI also claimed that the company had sold the tool to the FBI without explaining how it worked (that is, what vulnerability it exploited), so

[13] Citizen Lab, "The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender" (Aug. 24, 2016), https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/; Citizen Lab, "Reckless Redux: Senior Mexican Legislators and Politicians Targeted with NSO Spyware" (June 29, 2017), https://citizenlab.org/2017/06/more-mexican-nso-targets/; Nicole Perlroth, "Spyware's Odd Targets: Backers of Mexico's Soda Tax," The New York Times (Feb. 11, 2017), https://www.nytimes.com/2017/02/11/technology/hack-mexico-soda-tax-advocates.html; Azam Ahmed and Nicole Perlroth, "Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families," The New York Times (June 19, 2017), https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html; David Agren, "Mexican Spy Scandal Escalates as Study Shows Software Targeted Opposition," The Guardian (June 30, 2017), https://www.theguardian.com/world/2017/jun/30/mexico-spying-scandal-pegasus-opposition.

the FBI *couldn't* disclose the vulnerability to Apple because the FBI itself did not know it. The company thus got paid hundreds of thousands of dollars of U.S. taxpayers' money while retaining the ability to re-sell the same vulnerability to other buyers, with Apple left in the dark about how to patch it.[14]

The FBI's willingness to pay a steep price tag, without even getting full information about the vulnerability in exchange, signals to 0-day vendors that (at least in high-value cases) the U.S. government is willing to let 0-day vendors dictate the terms, including contractual or other limitations that undermine the government's own VEP policy. That is, not only are 0-day vendors not a reliable check on government abuses, they may also keep a government from following its own procedures for *preventing* abuse and ensuring responsible vulnerability disclosure to the flawed product's vendor at the appropriate time.

3. Attackers Co-opt Hacking Tools Over Which Governments Have Lost Control

The government sometimes loses control over its hacking tools, leading attackers to gain possession of those tools. A government may lose control of its tools several ways: through careless security practices, if an insider leaks or sells the tools, or if the government itself is hacked. Once a hacking tool has been disclosed outside the government's control, malicious actors have a window of opportunity to use it until the vendor of the affected software or hardware (from whom the government may have kept the vulnerability secret) can issue a patch and at-risk computer systems can be updated.

The U.S. government has experienced multiple high-profile incidents of hacking tool loss in recent years. In 2016, a hacker or group of hackers calling itself the Shadow Brokers offered to sell numerous top-secret NSA hacking tools online. The Shadow Brokers apparently obtained the malware from an external NSA "staging server" which the group had hacked around late 2013.[15] Following their initial attempts to sell the exploits, the Shadow Brokers dumped dozens of NSA hacking tools online for free in April 2017.[16]

The Shadow Brokers' disclosure of American intelligence agencies' hacking techniques had wide-reaching negative impacts on computer systems around the globe. One NSA tool called EternalBlue, which exploited a flaw in Microsoft software, was repurposed into a virulent piece of ransomware called WannaCry. WannaCry infected hundreds of thousands of computer systems worldwide in May

[14] *See* Knake, *supra* n.3.

[15] Bruce Schneier, "Who Are the Shadow Brokers?", *The Atlantic* (May 23, 2017), https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/.

[16] Scott Shane, "Malware Case Is Major Blow for the N.S.A.," *The New York Times* (May 16, 2017), https://www.nytimes.com/2017/05/16/us/nsa-malware-case-shadow-brokers.html.

2017.[17]

The very next month, another malware attack began spreading internationally after initially hitting critical infrastructure in Ukraine. NotPetya is thought to have begun as a Russian attack on Ukrainian government and infrastructure that wound up having a global impact.[18] Malware researchers established that, like WannaCry, NotPetya also made use of EternalBlue. NotPetya's creators leveraged the EternalBlue exploit, as well as another NSA exploit (called EternalRomance) also obtained by the Shadow Brokers,[19] and combined the techniques as part of NotPetya's sophisticated mechanism for spreading through networks.[20]

WannaCry and NotPetya infected such crucial systems as hospitals, power companies, shipping, and banking, endangering human life as well as economic activity. This shows that attackers, like governments, cannot entirely control which systems end up getting compromised.

The NSA is not the only U.S. intelligence agency to have lost control over its hacking tools. In March 2017, WikiLeaks released thousands of pages of Central Intelligence Agency (CIA) records documenting some of the CIA's hacking tools and techniques.[21]

[17] Bill Chappell, "WannaCry Ransomware: Microsoft Calls Out NSA for 'Stockpiling' Vulnerabilities," National Public Radio (May 15, 2017), https://www.npr.org/sections/thetwo-way/2017/05/15/528439968/wannacry-ransomware-microsoft-calls-out-nsa-for-stockpiling-vulnerabilities.

[18] *See* Nicholas Weaver, "Thoughts on the NotPetya Ransomware Attack," *Lawfare* (June 28, 2017), https://lawfareblog.com/thoughts-notpetya-ransomware-attack; Ellen Nakashima, "Ukraine's Ransomware Attack Was a Ruse to Hide Culprit's Identity, Researchers Say," The Washington Post (June 29, 2017), https://www.washingtonpost.com/world/national-security/this-weeks-global-ransomware-attack-was-a-ruse-to-deflect-attention-from-the-true-culprit-researchers-say/2017/06/29/da455a0e-5cf0-11e7-9b7d-14576dc0f39d_story.html.

[19] Microsoft, "New Ransomware, Old Techniques: Petya Adds Worm Capabilities," Microsoft Windows Security blog (June 27, 2017), https://blogs.technet.microsoft.com/mmpc/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/ (describing NotPetya's use of both EternalBlue and second NSA exploit dubbed EternalRomance).

[20] Lily Hay Newman, "A Scary New Ransomware Outbreak Uses WannaCry's Old Tricks," *Wired* (June 27, 2017), https://www.wired.com/story/petya-ransomware-outbreak-eternal-blue/; Weaver, "Thoughts on the NotPetya Ransomware Attack," *supra* n.18. Initially mistaken for a variant on the already-known Petya ransomware, researchers began calling the malware NotPetya after it became clear the virus was distinct from Petya. Russell Brandom, "A New Ransomware Attack Is Infecting Airlines, Banks, and Utilities Across Europe," The Verge (June 27, 2017), https://www.theverge.com/2017/6/27/15879480/petrwrap-virus-ukraine-ransomware-attack-europe-wannacry; Iain Thomson, "Everything You Need to Know About the Petya, Er, NotPetya Nasty Trashing PCs Worldwide," *The Register* (June 28, 2017), https://www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware/.

[21] Scott Shane, Matthew Rosenberg, and Andrew W. Lehren, "WikiLeaks Releases Trove of Alleged C.I.A. Hacking Documents," *The New York Times* (Mar. 7, 2017), https://www.nytimes.com/2017/03/07/world/europe/wikileaks-cia-hacking.html.

Among these was an exploit for a critical vulnerability in Cisco routers and switches. Following the WikiLeaks dump, Cisco issued a warning to its customers and stated there was no patch for the flaw at that time, though it said it was not aware of any malicious use of the vulnerability,[22] and it did release patches shortly thereafter.[23] WikiLeaks published additional CIA hacking tool documentation in June 2017.[24]

In another example, after nation-state actors widely believed to be the United States and Israel unleashed the so-called Stuxnet malware to undermine Iran's nuclear program, new malware which was in part identical to the Stuxnet code appeared on the internet.[25] Researchers also discovered additional types of malware that used Stuxnet's USB port infection technique to spread to computers.[26]

These incidents demonstrate that at the very least, to avoid compounding the problems that tool loss causes, governments need to know when vulnerability information is stolen and respond appropriately. By alerting affected vendors of vulnerabilities when the government's tools "escape," the government can mitigate the severity of attacks that use those vulnerabilities. But that post-tool-loss notification will not necessarily preclude the attacks entirely. The Shadow Brokers made an advance announcement of what NSA Windows tools they had obtained before releasing them, enabling NSA to notify Microsoft, so Microsoft had already issued patches for the vulnerabilities a month before the Shadow Brokers' release.[27] Nonetheless, because not all Windows users had patched their systems yet, WannaCry and NotPetya were still able to spread.

The government's demonstrated inability to retain exclusive control over its tools weakens one of the principal policy arguments in favor of government hacking. That argument is that government hacking is a preferable alternative to crypto backdoors because attacks on endpoints are ostensibly used judiciously against specific targets, whereas backdoors undermine security broadly for all users of the compromised encryption software. But when the government cannot maintain control over its

[22] Tom Spring, "Cisco Warns of Critical Vulnerability Revealed in 'Vault 7' Data Dump," ThreatPost (Mar. 20, 2017), https://threatpost.com/cisco-warns-of-critical-vulnerability-revealed-in-vault-7-data-dump/124414/.

[23] Doug Olenick, "Cisco Patches Vault 7 Vulnerability," SC Media US (May 10, 2017), https://www.scmagazine.com/cisco-patches-vault-7-vulnerability/article/656178/.

[24] Iain Thomson, "WikiLeaks Doc Dump Reveals CIA Tools for Infecting Air-Gapped PCs," *The Register* (June 22, 2017), https://www.theregister.co.uk/2017/06/22/wikileaks_cia_brutal_kangaroo/.

[25] "W32.Duqu: The Precursor to the Next Stuxnet", Symantec Official Blog (Oct. 18, 2011), https://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet

[26] Dennis Fisher, "New Gauss Malware, Descended From Flame and Stuxnet, Found On Thousands of PCs in Middle East", ThreatPost (August 9, 2012), https://threatpost.com/new-gauss-malware-descended-flame-and-stuxnet-found-thousands-pcs-middle-east-080912/76892/

[27] Dan Goodin, "Mysterious Microsoft Patch Killed 0-Days Released by NSA-Leaking Shadow Brokers," Ars Technica (Apr. 15, 2017), https://arstechnica.com/information-technology/2017/04/purported-shadow-brokers-0days-were-in-fact-killed-by-mysterious-patch/.

exploits, hacking looks less like a targeted sniper's bullet and more like a poorly-aimed bomb, with a broad and indiscriminate blast radius.

After two worldwide malware attacks in as many months in 2017, the NSA started to experience political blowback for building a cache of powerful tools it cannot keep safe.[28] One former director of the NSA has said, in the wake of the WannaCry attack, that he cannot defend an agency's having powerful hacking tools if it can't protect them and keep them from falling into the wrong hands.[29]

Even assuming the U.S. or other governments can be trusted to use endpoint hacking sparingly against relatively few, legitimately-chosen targets, incidents such as WannaCry and NotPetya show that governments are not capable of limiting those tools to those intentional use cases. This is a serious drawback that cannot be overlooked in debating the viability of government hacking as a "middle ground" alternative to encryption backdoors.

4. Attackers Learn of Vulnerabilities Through Government Use of Malware

Attackers may obtain government malware through the government's intentional deployment of a hacking tool against a target. The vulnerability that a government hacking tool relies on is exposed as soon as that software is deployed. That is because one can obtain a copy of the malware from a target device and examine the code to learn how the program works. This analysis allows one to identify the flaw that enabled the software to infect the target machine. Once the vulnerability is identified, a malicious actor can create a program to exploit the same flaw. Alternatively, an attacker could simply repurpose the original exploit code and deploy it against other targets (as discussed above regarding the WannaCry and NotPetya malware).

Once it has been discovered, government-deployed malware can kick off a race between attackers and defenders. The vendor of the affected software strives to patch the vulnerability exploited by the government before malicious actors can use it. For example, in the fall of 2016, a child pornography site called "GiftBox" began infecting visitors' Tor browsers with malware that used a 0-day exploit of a flaw in the Tor browser. Multiple people quickly analyzed the malware, and determined

[28] Nicole Perlroth and David E. Sanger, "Hacks Raise Fear Over N.S.A.'s Hold on Cyberweapons," The New York Times (June 28, 2017), https://www.nytimes.com/2017/06/28/technology/ransomware-nsa-hacking-tools.html.

[29] *See* Shane, "Malware Case Is Major Blow for the N.S.A.," *supra* n.16 (quoting Gen. Michael V. Hayden). However, another ex-NSA director defended the NSA's tools, claiming the NSA eventually discloses 90% or more of the exploits the agency "gets." Natasha Lomas, "After WannaCry, Ex-NSA Director Defends Agencies Holding Exploits," TechCrunch (May 16, 2017), https://techcrunch.com/2017/05/16/after-wannacry-ex-nsa-director-defends-agencies-holding-exploits/ (quoting Gen. Keith Alexander).

that French law enforcement was likely behind it. The Tor Project, which maintains the Tor browser, and Mozilla, which maintains the Firefox browser (off which the Tor browser is built), both issued patches very promptly. In the interim, it is possible that others were seeking to use the exploit before it got patched,[30] though that may be unlikely given that network defenders would be keeping an eye out for such activity.

Vendors' prompt response time is a mitigating factor for this particular risk of government hacking. But not every vulnerability can be patched by a vendor promptly (as with the aforementioned Cisco bug), or even at all. Even if a patch for the affected software exists, the device running the software may be un-patchable, leaving the owners of the device (say, an expensive MRI machine) to choose between continuing to run a vulnerable machine and impairing their operational capabilities by taking the machine out of service.[31]

At the same time, the very fact of patching can empower attackers. Attackers use patches as a guide to build exploits, working backwards from the patch to figure out what the vulnerability was. The resulting exploit won't affect patched systems, but as noted, many systems are not promptly, or ever, patched. Government disclosure of a vulnerability to a vendor thus can perversely result in a scenario where the disclosure can enable an attacker. That is, there are risks both if law enforcement chooses to disclose the vulnerability to a vendor, and if law enforcement chooses to exploit it offensively in a government hacking operation. Attackers may learn about the exploit either way. Many security experts agree that in most situations, disclosure is nevertheless worth the risk that an attacker will reverse-engineer the patch to build an exploit.[32]

In short, the risks of government hacking and vulnerability disclosure or nondisclosure do not arise in isolation; they interplay in complex ways.

5. Government Incentives to Push for Less-Secure Software and Standards

When investigating crime, terrorism, or espionage, the government understandably wants to work efficiently. In a government hacking campaign, the easier it is for government agents to hack the targeted software or hardware, the less time,

[30] Nicholas Weaver, "The End of the NIT," Lawfare (Dec. 5, 2016), https://www.lawfareblog.com/end-nit; Joseph Cox and Lorenzo Franceschi-Bicchierai, "Newly Uncovered Tor Browser Exploit Targeted Dark Web Child Porn Site," Motherboard (Nov. 30, 2016), https://motherboard.vice.com/en_us/article/9a3mq7/tor-browser-zero-day-exploit-targeted-dark-web-child-porn-site-giftbox.

[31] John E. Dunn, "Imagine you're having a CT scan and malware alters the radiation levels – it's doable," The Register (Apr. 11, 2018), https://www.theregister.co.uk/2018/04/11/hacking_medical_devices/.

[32] *See, e.g.*, Steven M. Bellovin, Matt Blaze, Sandy Clark, & Susan Landau, *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 Nw. J. Tech. & Intell. Prop. 1, 53 (2014).

resources, and personnel will have to be expended. However, the desire for efficiency risks incentivizing the government to push vendors to make or keep their software less secure, and to push standards-setting bodies charged with protecting information security to adopt weakened standards that undermine security instead.

For example, the NSA has subverted cryptographic standards and software for its own advantage. The NSA has dual missions: one defensive (protecting vital U.S. systems and information), one offensive (intelligence-gathering).[33] The former lost out to the latter when, in 2006, the NSA secretly convinced the National Institute for Standards and Technology (NIST) to insert a backdoor into an algorithm for pseudorandom number generation called Dual_EC_DRBG.[34] NIST is responsible, among other things, for developing cryptographic standards and guidelines, including approving cryptographic algorithms on which private- and public-sector entities in the U.S. and worldwide rely to secure sensitive information. But in the case of Dual_EC_DRBG, that reliance proved misplaced after the NSA's actions came to light as part of the 2013 Snowden revelations. As cryptographer Matthew Green explained, the Dual_EC_DRBG backdoor "may allow the NSA to break nearly any cryptographic system that uses it."[35] Among those systems was BSafe, a software product made by well-respected encryption company RSA. At the end of 2013, additional Snowden documents revealed a secret contract for the NSA to pay RSA $10 million to use the weakened Dual_EC_DRBG standard in BSafe,[36] thereby potentially opening up all of RSA's BSafe customers to NSA snooping.

Another company that used Dual_EC_DRBG was Juniper Networks. In December 2015, Juniper announced that it had found "unauthorized code" in ScreenOS, the embedded operating system for Juniper's hardware firewall devices: a malicious backdoor that automatically decrypted VPN traffic, which had been lurking in the software for three years.[37] Juniper had used a modified version of NIST's backdoored Dual_EC_DRBG standard for ScreenOS. ScreenOS retained the backdoored random number generator, but changed a particular constant ("Q") in the generator to Juniper's own Q value, replacing the NSA-chosen original Q in the NIST standard.

[33] *See* National Security Agency, Frequently Asked Questions, https://www.nsa.gov/about/faqs/about-nsa-faqs.shtml (describing these "two interconnected missions").

[34] Matthew Green, "The Many Flaws of Dual_EC_DRBG," A Few Thoughts on Cryptographic Engineering blog (Sept. 18, 2013), https://blog.cryptographyengineering.com/2013/09/18/the-many-flaws-of-dualecdrbg/.

[35] *Id.*

[36] Russell Brandom, "NSA Paid $10 Million to Put Its Backdoor in RSA Encryption, According to Reuters Report," The Verge (Dec. 20, 2013), https://www.theverge.com/2013/12/20/5231006/nsa-paid-10-million-for-a-back-door-into-rsa-encryption-according-to.

[37] Kim Zetter, "Secret Code Found in Juniper's Firewalls Shows Risk of Government Backdoors," Wired (Dec. 18, 2015), https://www.wired.com/2015/12/juniper-networks-hidden-backdoors-show-the-risk-of-government-backdoors/; Bruce Schneier, "Back Door in Juniper Firewalls," Schneier on Security (Dec. 21, 2015), https://www.schneier.com/blog/archives/2015/12/back_door_in_ju.html.

Unknown hackers somehow replaced Juniper's Q with their own Q in Juniper's ScreenOS code. To quote cryptographer Matt Green, "To sum up, some hacker or group of hackers noticed *an existing backdoor* in the Juniper software, ... then piggybacked on top of it to build a backdoor of their own, something they were able to do because … Juniper had already paved the road" by using a backdoored algorithm. "The end result," Green explains, "was a period in which someone—maybe a foreign government—was able to decrypt Juniper traffic in the U.S. and around the world."[38]

The Dual_EC_DRBG story shows that there isn't a bright line between crypto backdoors and government hacking. The U.S. government pushes for deliberately weakened software and standards (backdoors) in order to facilitate its hacking activities. Since "it's awfully hard to control" a cryptographic backdoor once it's been deployed,[39] intentionally-weakened standards, besides being problematic on their own, also exacerbate the risks of government hacking.

6. Government Malware Affects Innocent Users

Finally, when law enforcement compromises a computer system, the malware it installs could affect innocent users by gathering data about or getting onto the computers of innocent people using the compromised system.

In 2013, an effort by the FBI to identify people suspected of trading child exploitation images impacted innocent people using the same computer servers, all of which were hosted by a company called Freedom Hosting. Freedom Hosting made it easy to have a "Tor hidden service" site that would hide the website's true geographic location, and which could be reached only over the Tor anonymity network. Tor hidden services are used by sites that need to evade surveillance or protect users' privacy to an extraordinary degree – including human rights groups and journalists. They are also used by child-pornography traders.

To identify the child-pornography traders, it appears the FBI gained control of the Freedom Hosting servers through a Mutual Legal Assistance request to France, where the company leased its machines.[40] Soon thereafter, the FBI used malware,

[38] Matthew Green, "On the Juniper Backdoor," A Few Thoughts on Cryptographic Engineering (Dec. 22, 2015), https://blog.cryptographyengineering.com/2015/12/22/on-juniper-backdoor/. *See also* Matthew Green, "Applied Kleptography," talk given at Univ. of Michigan Dept. of Computer Science & Engineering Security Seminar (Apr. 4, 2017), *slides available at* https://www.dropbox.com/s/hhtnhef8zuc3yo5/AppliedKleptography.pdf?dl=0 (describing NSA's undermining of the Dual_EC_DRBG standard and the subsequent ScreenOS incident).

[39] Matthew Green, "The Strange Story of 'Extended Random,'" A Few Thoughts on Cryptographic Engineering blog (Dec. 19, 2017), https://blog.cryptographyengineering.com/2017/12/19/the-strange-story-of-extended-random/.

[40] Kevin Poulsen, "If You Used This Secure Webmail Site, the FBI Has Your Inbox," *Wired* (Jan. 24, 2014), https://www.wired.com/2014/01/tormail/.

which it called a “network investigative technique” or “NIT,” on all of Freedom Hosting’s hidden service sites. The maintenance page included source code that exploited a critical memory management vulnerability in the Firefox browser, specifically targeting the version of Firefox that forms the basis of the Tor browser. In other words, the attack was focused specifically on deanonymizing Tor users.[41]

However, the NIT appears to have been served to the Tor browsers of anyone who visited a site hosted on Freedom Hosting’s seized servers.[42] Those sites included an anonymous webmail service called TorMail, which was used by criminals, but also by journalists, activists, and dissidents.[43] The campaign to unmask suspected criminals thus deanonymized journalists, dissidents, and other innocent individuals who hid their identities through the service.

In a similar case, the FBI took over another server suspected of hosting child exploitation material on a site called “Playpen.” The FBI again deployed a NIT from the Playpen site to determine site visitors’ true IP addresses by exploiting an undisclosed flaw in the Tor browser. This time, the FBI apparently learned from its experience in Freedom Hosting: it allegedly took some steps to limit infections with the NIT by installing it on users’ browsers only after the user had logged into the site with a username and password.[44] That is, the NIT was ostensibly deployed from a part of the site that a user was unlikely to stumble upon without some interest in photographs of sexual exploitation of children.

By failing to narrowly tailor its use of NITs in the Freedom Hosting case, the FBI undoubtedly swept in people who had not committed or attempted to commit any crime. The FBI placed malware on innocent individuals’ computers and gathered data about them, including information the users had tried to mask by using Tor.[45] Yet unless they were subsequently indicted, there is no indication that the FBI notified affected individuals that it had hacked their computers. The users would not know that there was malware on their computers or how to remove it, or that Tor’s security functionality did not work as they believed.

[41] Kevin Poulsen, “FBI Admits It Controlled Tor Servers Behind Mass Malware Attack,” *Wired* (Sept. 13, 2013), https://www.wired.com/2013/09/freedom-hosting-fbi/.

[42] Lorenzo Franceschi-Bicchierai, “The FBI Hacked a Dark Web Child Porn Site to Unmask Its Visitors,” *Motherboard* (Jul. 15, 2015), https://motherboard.vice.com/en_us/article/mgbygy/the-fbi-hacked-a-dark-web-child-porn-site-to-unmask-its-visitors.

[43] Alyssa Hertig, “FBI ‘Incidentally’ Seized Entire TorMail Email Server,” Reason (Jan. 28, 2014), https://reason.com/blog/2014/01/28/fbi-incidentally-seized-entire-tormail-e.

[44] Compare the search warrant for the Freedom Hosting NIT, *available at* https://www.documentcloud.org/documents/3217570-Freedom-Hosting-Returned-Warrant.html (referring to deployment of NIT “on the computer server”), with the search warrant application for the Playpen NIT, *available at* https://www.documentcloud.org/documents/2166606-ferrell-warrant-1.html#document/p11/a227236 (referring to deployment of NIT solely on “Website A,” *i.e.*, Playpen).

[45] *See* NIT warrant application, *supra* n.44, at 12 (listing all the data the NIT collected).

Government hacking affects innocent users, but those users may never know it. Judges issue hacking warrants *ex parte* based on the assurances of the government, but those representations may not capture the hacking campaign's impact on people for whom there is no probable cause to believe they have committed any crime. As its use of hacking techniques continues and expands, it will be important for the government to narrowly tailor hacking campaigns to minimize impact on innocent users and to explain the expected impact accurately to the authorizing judge.

C. Conclusion

Government hacking is often lauded as a solution to the "going dark" problem. It is too dangerous to mandate encryption backdoors, but targeted hacking of endpoints could ensure investigators access to same or similar necessary data with less risk. Vulnerabilities will never affect everyone, contingent as they are on software, network configuration, and patch management. Backdoors, however, mean everybody is vulnerable and a security failure fails catastrophically. In addition, backdoors are often secret, while eventually, vulnerabilities will typically be disclosed and patched.

The premise of the panel CIS and Mozilla convened in February 2017, and of this paper, is that the risk of government hacking compared to an access mandate is relatively under-examined. We should not take it on faith that government hacking is a safe practice. This is why we need more discussion and research on the security risks from government hacking. Our February 2017 panel, and this paper, are meant as a starting point for further work as the national, indeed global, debate over encryption and law enforcement powers continues.

Acknowledgements

CIS wishes to thank our February 2017 panel members for their invaluable contributions to this important topic: Prof. Dan Boneh, Dr. Sandy Clark, Richard Barnes, Oren Falkowitz, Stephan Somogyi, and Logan Brown. Thank you to Nicholas Weaver for his valuable input on an earlier draft of this paper, and to Jennifer Granick for her contributions to the final product.

CIS is grateful to Mozilla for co-sponsoring our event series on government hacking, as well as to the Stanford Cyber Initiative for providing additional funding assistance. A full list of CIS funders is available at https://cyberlaw.stanford.edu/about-us. This paper is a publication of CIS and does not reflect the opinions of any of the funders of the event series or of CIS.

About the Author

Riana Pfefferkorn is the Cryptography Fellow at the Stanford Center for Internet and Society. Her work, made possible through funding from the Stanford Cyber Initiative, focuses on investigating and analyzing the U.S. government's policy and practices for forcing decryption and/or influencing the encryption-related design of online platforms and services, devices, and products, both via technical means and through the courts and legislatures. Riana also researches the benefits and detriments of strong encryption on free expression, political engagement, economic development, and other public interests. Prior to joining Stanford, Riana was an associate in the Internet Strategy & Litigation group at the law firm of Wilson Sonsini Goodrich & Rosati, and the law clerk to the Honorable Bruce J. McGiverin of the U.S. District Court for the District of Puerto Rico. She is a graduate of the University of Washington School of Law and Whitman College.

About the Center for Internet and Society

The Center for Internet and Society (CIS) is a public interest technology law and policy program at Stanford Law School and a part of Law, Science and Technology Program at Stanford Law School. CIS brings together scholars, academics, legislators, students, programmers, security researchers, and scientists to study the interaction of new technologies and the law and to examine how the synergy between the two can either promote or harm public goods like free speech, innovation, privacy, public commons, diversity, and scientific inquiry. CIS strives to improve both technology and law, encouraging decision makers to design both as a means to further democratic values. CIS provides law students and the general public with educational resources and analyses of policy issues arising at the intersection of law, technology and the public interest. CIS also sponsors a range of public events including a speakers series, conferences and workshops. CIS was founded by Lawrence Lessig in 2000.