Law Enforcement Using and Disclosing Technology Vulnerabilities

Kristin Finklea
Specialist in Domestic Security

April 26, 2017

Congressional Research Service
7-5700
www.crs.gov
R44827

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

There has been increased discussion about law enforcement legally "hacking" and accessing certain information about or on devices or servers. Law enforcement has explored various avenues to discover and exploit vulnerabilities in technology so it may attempt to uncover information relevant to a case that might otherwise be inaccessible. For instance, as people have adopted tools to conceal their physical locations and anonymize their online activities, law enforcement reports that it has become more difficult to locate bad actors and attribute certain malicious activity to specific persons. As a result, officials have debated the best means to obtain information that may be beneficial to the administration of justice. Exploiting vulnerabilities is one such tool.

Law enforcement's use of tools that take advantage of technology vulnerabilities has evolved over the years. The first reported instances of law enforcement hacking involved authorities using keylogging programs to obtain encryption keys and subsequent access to devices. More recently, law enforcement has been relying on specially designed exploits, or network investigative techniques (NITs), to bypass anonymity protections of certain software. In addition, investigators have leveraged vulnerabilities discovered in software designed to encrypt or otherwise secure data and limit access to information.

In exploiting vulnerabilities, law enforcement may leverage previously *known* vulnerabilities that have not yet been patched. Alternatively, it may develop tools to detect and take advantage of previously *unknown* and *undisclosed* vulnerabilities. It is law enforcement's use and disclosure of these previously unknown vulnerabilities that has become the subject of some debate.

The Obama Administration established a process, known as the Vulnerabilities Equities Process (VEP), to help decide whether or not to disclose information about newly discovered vulnerabilities. The VEP is triggered whenever a federal government entity, including law enforcement, discovers or obtains a new hardware or software vulnerability. The discussion on whether the government, and law enforcement, should generally retain or disclose discovered vulnerabilities lacks a number of data points that may help inform the conversation. For example, in what number or proportion of cases does law enforcement leverage technology vulnerabilities to obtain evidence? Are there tools other than vulnerability exploits or NITs that law enforcement can use to obtain the same evidence, and how often are those tools utilized?

Congress may examine a range of policy issues related to law enforcement using and disclosing vulnerabilities. For example, how does law enforcement's ability to lawfully hack, or exploit vulnerabilities, influence the current debate surrounding whether law enforcement is "going dark," or being outpaced by technology? In addition, how does law enforcement acquire the knowledge of vulnerabilities and associated exploits? Might law enforcement consider establishing its own (or supporting others') reward programs in order to gain knowledge of vulnerabilities or exploits? Given the current VEP framework, is it the most effective method for law enforcement to use in determining whether to share vulnerability information with the technology industry, and how might law enforcement share such information with their multilateral law enforcement partners?

Contents

Contacts

There has been increased discussion about law enforcement legally "hacking" and accessing certain information on or about devices or servers. Officials conduct this hacking as part of criminal investigations and takedowns of websites that host illicit content or facilitate illegal activity. There have been reports of such hacking for more than a decade.[1]

Over the years, law enforcement has explored various avenues to discover and exploit vulnerabilities in technology so it may attempt to uncover information relevant to a case that might otherwise be inaccessible. For instance, as people have adopted tools to conceal their physical locations and anonymize their online activities, law enforcement reports that it has become more difficult to locate bad actors and attribute certain malicious activity to specific persons. As a result, officials have debated the best route to access information that may be beneficial to the administration of justice. Exploiting vulnerabilities is one such tool.

In exploiting vulnerabilities, law enforcement may take one of two broad paths to gain access to devices and information. It may rely upon known vulnerabilities that have not yet been patched, or it may develop tools to detect and use previously unknown and undisclosed vulnerabilities (or otherwise acquire exploits for these zero-day vulnerabilities) that it can then leverage.[6]

Law enforcement's use of previously unknown vulnerabilities has become the subject of some debate. Policymakers have questioned law enforcement practices for maintaining versus disclosing these vulnerabilities. They have also questioned how maintaining or disclosing vulnerabilities may impact security—information security, public safety, and homeland security alike. This has opened a broader debate about whether law enforcement *should* disclose vulnerabilities and whether there should be rules for law enforcement behavior in this arena.

This report provides background on law enforcement's use of technology vulnerabilities in criminal investigations. It

Relevant Terms

Defining several terms may help facilitate the current discussion surrounding law enforcement's use and disclosure of vulnerabilities in technology:

Encryption: a process to secure information by converting it from a state that can be read to that which cannot be read without a "key."[2]

Exploit: software, malware, or commands that can be used to take advantage of vulnerabilities in technology.[3]

Malware: "malicious software" such as a worm, virus, trojan, or spyware designed to take advantage of technology vulnerabilities or make changes to the normal operation of a device without the owner's knowledge.

Network investigative technique (NIT): law enforcement's term for a specially designed exploit or malware engineered to take advantage of a specific technology vulnerability.[4]

Vulnerability: a security hole or weakness in hardware, software, or firmware that can leave it open to becoming compromised.

Zero-day vulnerability: a vulnerability "that is yet unknown to the software maker or to antivirus vendors. This means the vulnerability is also not yet publicly known.... The term 'zero-day' refers to the number of days that the software vendor has known about the hole."[5]

[1] Kevin Poulsen, "FBI Admits It Controlled Tor Servers Behind Mass Malware Attack," *Wired.com*, September 13, 2013.

[2] For a technical explanation of encryption, see CRS Report R44642, *Encryption: Frequently Asked Questions*.

[3] For more information about exploits and vulnerabilities, see Internet Corporation for Assigned Names and Numbers, *Threats, Vulnerabilities, and Exploits - Oh My!*, August 10, 2015.

[4] Kevin Poulsen, "Visit The Wrong Website and The FBI Could End Up In Your Computer," *Wired*, August 5, 2014.

[5] Kim Zetter, "Hacker Lexicon: What is a Zero Day?," *Wired*, November 11, 2014.

[6] Ahmed Ghappour, "Is the FBI Using Zero-Days in Criminal Investigations?," *Just Security*, November 17, 2015.

also provides information on the government's system by which agencies collectively determine whether to maintain or disclose newly discovered vulnerabilities. The report also outlines a range of policy issues that may arise regarding the use and disclosure of vulnerabilities in technology.[7]

Evolution of Law Enforcement Exploiting Vulnerabilities

The first reported instances of law enforcement hacking involved authorities using keylogging programs to obtain encryption keys and subsequent access to devices. For example, in a 1999 case against a Cosa Nostra mob boss the Federal Bureau of Investigation (FBI) physically installed a keylogger[8] (using a technique that was classified at the time) on his computer to capture his encryption key and gain access to his computer.[9] Several years later, in 2001, authorities started using a more advanced keylogger—one that could be installed remotely—named Magic Lantern. In addition to capturing keystrokes, Magic Lantern could record Internet browsing histories and usernames/passwords for sites.[10]

More recently, law enforcement has been utilizing exploits to bypass protections of software such as Tor,[11] which allows users to access websites anonymously. In addition, it has relied on vulnerabilities discovered in software that encrypts or otherwise secures data and limits access to information. While some investigations are known to have used specially designed exploits or malware, referred to as Network Investigative Techniques (NITs), others are merely suspected of using NITs to exploit vulnerabilities. The remainder of this section discusses examples of how the FBI has utilized exploits or malware over the years to facilitate its investigations.

[7] Notably, there have been questions regarding potential privacy concerns of law enforcement using vulnerabilities. However, some have posited that the debate should not necessarily be framed as privacy versus security, but rather security versus security. See, for instance, testimony by Susan Landau before U.S. Congress, House Committee on the Judiciary, *The Encryption Tightrope: Balancing Americans' Security and Privacy*, 114th Cong., 2nd sess., March 1, 2016. The privacy discussion, however, is beyond the scope of this report. For more information about privacy of stored and electronic communications, see CRS Report R44036, *Stored Communications Act: Reform of the Electronic Communications Privacy Act (ECPA)*. For information about pitting privacy against security in the context of law enforcement investigations, see CRS Report R44481, *Encryption and the "Going Dark" Debate*. For more information about privacy of stored and electronic communications, see CRS Report R44036, *Stored Communications Act: Reform of the Electronic Communications Privacy Act (ECPA)*.

[8] A keylogger is a program or device that will record the keystrokes that are entered on a computer keyboard.

[9] Kim Zetter, "Everything We Know About How the FBI Hacks People," *Wired*, May 15, 2016. See also Sayako Quinlan and Andi Wilson, *A Brief History of Law Enforcement Hacking in the United States*, New America, September 2016.

[10] Ibid.

[11] For more information on Tor (short for The Onion Router), see the text box, "Tor and the Dark Web." Tor "refers both to the software that you install on your computer to run Tor and the network of computers that manages Tor connections." Adam Clark Estes, "Tor: The Anonymous Internet, and If It's Right for You," *Gizmodo*, August 30, 2013.

Tor and the Dark Web[12]

The layers of the Internet go far beyond the surface content that many can easily access in their daily searches. The other content is that of the *Deep Web*, content that has not been indexed by traditional search engines such as Google. The furthest corners of the Deep Web, segments known as the *Dark Web*, contain content that has been *intentionally* concealed. The Dark Web may be used for legitimate purposes as well as to conceal criminal or otherwise malicious activities.

The Dark Web can be reached through decentralized, anonymized nodes on a number of networks including Tor (short for The Onion Router).[13] Tor was originally created by the U.S. Naval Research Laboratory as a tool for anonymously communicating online. Its users connect to websites "through a series of virtual tunnels rather than making a direct connection, thus allowing both organizations and individuals to share information over public networks without compromising their privacy."[14] Users route their web traffic through other users' computers such that the traffic cannot be traced to the original user. Tor essentially establishes layers (like layers of an onion) and routes traffic through those layers to conceal users' identities.[15] To get from layer to layer, Tor has established "relays" on computers around the world through which information passes. Information is encrypted between relays, and "all Tor traffic passes through at least three relays before it reaches its destination."[16] The final relay is called the "exit relay," and the Internet Protocol (IP) address of this relay is viewed as the source of the Tor traffic. When using Tor software, users' IP addresses remain hidden. As such, it appears that the connection to any given website "is coming from the IP address of a Tor exit relay, which can be anywhere in the world."[17]

Operation Torpedo

In 2011, the Netherlands' National High Tech Crime Unit began an investigation into child pornography websites hosted on the Dark Web. During the course of this investigation, they learned[18]—and informed the FBI—that a server hosting one of these sites was located in Nebraska. The FBI then traced the server's IP address to Aaron McGrath, who they later arrested. They also seized the servers.

The FBI's affidavit supporting its search warrant application detailed the purpose of the NIT it proposed to use in its investigation.[19] The FBI believed that the NIT was the "only available investigative technique with a reasonable likelihood of securing the evidence necessary to prove beyond a reasonable doubt the actual location and identity of those users" viewing certain pages of the child pornography websites administered by McGrath or sending/viewing private messages on those pages.[20]

[12] For more information, see CRS Report R44101, *Dark Web*.

[13] More information on Tor is available at https://www.torproject.org/. Tor is the most widely used anonymous network.

[14] Tor Project, *Tor: Overview*, https://www.torproject.org/about/overview.html.en.

[15] Adam Clark Estes, "Tor: The Anonymous Internet, and If It's Right for You," *Gizmodo*, August 30, 2013.

[16] Electronic Frontier Foundation, *What is a Tor Relay?*, https://www.eff.org/pages/what-tor-relay.

[17] Ibid. According to the Electronic Frontier Foundation, "[a]n exit relay is the final relay that Tor traffic passes through before it reaches its destination. Exit relays advertise their presence to the entire Tor network, so they can be used by any Tor users. Because Tor traffic exits through these relays, the IP address of the exit relay is interpreted as the source of the traffic."

[18] Reportedly, they determined this because the administrator account for the website had not been password protected. See Kevin Poulsen, "Visit The Wrong Website and The FBI Could End Up In Your Computer," *Wired*, August 5, 2014.

[19] *In the Matter of the Search of Computers that Access the Website 'Bulletin Board A'* (United States District Court for the District of Nebraska 2012).

[20] Ibid., p. 30.

The NIT was proposed to direct relevant computers accessing three specific child pornography websites to download instructions that would direct the computer to send certain information (computer identifying information, location, and user) back to the FBI. The FBI specified that the NIT would not hinder the use or functionality of impacted computers.[21]

Through the use of the NIT, the FBI reportedly collected IP addresses of at least 25 U.S. visitors to the child pornography websites. The FBI then subpoenaed the Internet Service Providers for the physical addresses of the computers associated with the IP addresses. The FBI was then able to make arrests around the country.

As experts have noted, this was "the first time—that we know of—that the FBI deployed such code broadly against every visitor to a website, instead of targeting a particular suspect."[22]

Seizure of Freedom Hosting

In 2013, the FBI seized Freedom Hosting, a website hosting service operating on the Tor network that was reportedly home to more than 40 child pornography websites, as well as additional sites with no links to child pornography.[23] When the FBI took control of the site, it infected it with "custom malware designed to identify visitors."[24] This custom malware "exploited a Firefox security hole to cause infected computers to reveal their real IP addresses to the FBI."[25] Specifically, the NIT targeted computers that accessed 23 specific websites on Freedom Hosting.[26] It also targeted users of specific Tor Mail email accounts—a "free, anonymous e-mail service provider that operates as a 'hidden service' on the Tor network"—that investigators had linked to child pornography crimes.[27]

Like in Operation Torpedo, the FBI's exploit against Freedom Hosting targeted all visitors to the associated websites—both illegal child pornography sites and legitimate businesses. As experts have noted, customers to the legitimate websites may have been impacted by the FBI's malware. Because the court documents have been sealed and the FBI has not discussed details of the exploit, it is unknown how many innocent individuals may have been "hooked" by the FBI's malware.[28]

Operation Pacifier

The FBI conducted an investigation into a child pornography website known as Playpen, which was operating on the Dark Web and had nearly 215,000 members.[29] Through the course of its investigation, the FBI determined that the computer server hosting Playpen was located in North Carolina.[30] In February 2015, the FBI seized this server, and subsequently continued to run the

[21] Ibid., p. 31.

[22] Kevin Poulsen, "The FBI Used the Web's Favorite Hacking Tool to Unmask Tor Users," *Wired*, December 16, 2014.

[23] Kevin Poulsen, "FBI Admits It Controlled Tor Servers Behind Mass Malware Attack," *Wired.com*, September 13, 2013.

[24] Ibid.

[25] Kim Zetter, "Everything We Know About How the FBI Hacks People," *Wired*, May 15, 2016.

[26] Affidavit in Support of Application for Search Warrant, *In the Matter of the Search of Computers that Access 'Websites 1-23'* (U.S. District Court for the District of Maryland).

[27] Ibid., p. 14.

[28] Kim Zetter, "Everything We Know About How the FBI Hacks People," *Wired*, May 15, 2016.

[29] *US v. Ferrell* (Affidavit in Support of Application for a Search Warrant 2015).

[30] The IP address, reportedly, was publicly available.

website for nearly two weeks from a server in Virginia.[31] In addition, a Virginia District Court judge authorized a search warrant allowing law enforcement to employ an NIT to try to identify actual IP addresses of computers used to access Playpen.

The NIT in the Playpen case sent a command to users' computers directing those computers to send certain information back to the FBI. This information included the computer's true IP address, a unique identifier that would distinguish it from other machines, and information on whether this computer had already received the NIT.[32]

Through the use of the NIT, the FBI was able to uncover about 1,300 IP addresses and subsequently trace those to individuals.[33] Criminal charges have been filed against more than 185 individuals.[34] The FBI has declined to reveal the details of the NIT used against the Playpen website,[35] and in at least one case has opted to dismiss charges rather than reveal the NIT source code.[36] The FBI has also classified elements of the NIT,[37] which, as experts have noted, impedes criminal discovery of the specific NIT source code.[38]

Operation Onymous

In November 2014, the FBI and over 15 countries, operating through the European Cybercrime Center (EC3), launched Operation Onymous to investigate several Dark Web markets that traded in drugs, weapons, credit card information, fake documents, and computer hacking tools, among other things.[39] Among the websites taken down in this operation was Silk Road 2, one of the most notorious online global bazaars for illicit services and contraband (mainly drugs).[40]

The Department of Justice (DOJ) noted that, "using court-authorized legal processes and Mutual Legal Assistance Treaty Requests, [international law enforcement] seized 400 online user addresses and multiple computer servers."[41] These addresses could be accessed via Tor. However, authorities did not reveal how they bypassed security and anonymity protections offered by Tor and specifically stated they were keeping that information secret.[42] Some speculate that the FBI

[31] *US v. Ferrell* (Affidavit in Support of Application for a Search Warrant 2015).

[32] *US v. Ferrell* (Affidavit in Support of Application for a Search Warrant 2015).

[33] Mary-Ann Russon, "FBI Crack Tor and Catch 1,500 visitors to Biggest Child Pornography Website on the Dark Web," *International Business Times*, January 6, 2016. Joseph Cox, "The FBI's 'Unprecedented' Hacking Campaign Targeted Over a Thousand Computers," *Motherboard*, January 5, 2016.

[34] Mike Carter, "Investigation of FBI's Child Pornography Operation Sparks Controversy Over Internet Privacy," *Government Technology*, August 31, 2016.

[35] Tim Cushing, "Judge Says the FBI Can Keep Its Hacking Tool Secret, But Not the Evidence Obtained With It," *techdirt*, May 27, 2016.

[36] See Government's Unopposed Motion to Dismiss Indictment Without Prejudice, *United States of America v. Jay Michaud*, (United States District Court for the Western District of Washington at Tacoma 2017).

[37] See Government's Response to Defendant's Motion to Compel, *United States of America v. Gerald Andrew Darby*, 22 (United States District Court for the Eastern District of Virginia 2016).

[38] Cyrus Farivar, "To Keep Tor Hack Source Code Secret, DOJ Dismisses Child Porn Case," *ArsTechnica*, March 5, 2017.

[39] Department of Justice, "Attorney General Loretta E. Lynch Delivers Remarks at RSA Conference on Cybersecurity," press release, March 1, 2016.

[40] See Andy Greenberg, "Global Web Crackdown Arrests 17, Seizes Hundreds of Dark Net Domains," *Wired*, November 7, 2014.

[41] Department of Justice, "Attorney General Loretta E. Lynch Addresses the European Cybercrime Center at Europol," press release, September 16, 2015.

[42] Andy Greenberg, "Global Web Crackdown Arrests 17, Seizes Hundreds of Dark Net Domains," *Wired*, November 7, (continued...)

may have paid Carnegie Mellon researchers for an exploit technique to take down certain dark websites. The FBI has not confirmed this, however, and has denied allegations that it paid $1 million to Carnegie Mellon for an exploit tool.[43]

San Bernardino iPhone

In addition to exploiting vulnerabilities in websites and networks to obtain information *about* certain devices, law enforcement has also leveraged weaknesses in hardware and software to access content *on* certain devices. In the aftermath of the December 2, 2015, San Bernardino, CA, terrorist attack, investigators recovered an Apple iPhone belonging to one of the shooters. Law enforcement hoped that the device would contain valuable information on who the shooters may have been communicating with to plan the attacks, where the shooters may have traveled prior to the attack, and the potential involvement of others in the attack.[44] However, after several months the FBI was still unable to access information on the device. The FBI requested through the courts that Apple assist investigators in accessing the data. Apple refused to comply. After a back and forth legal battle, the FBI ultimately found assistance from a third party entity, was able to access the contents of the phone, and dropped the case with Apple.[45] Specifically, the FBI paid hackers to find a software flaw that the bureau was then able to leverage to ultimately crack into the iPhone.[46]

Researchers have noted that the FBI has not disclosed to Apple information about vulnerabilities in its operating system software that were discovered and used to get into the San Bernardino iPhone.[47] Moreover, the FBI has noted that it *cannot* reveal the vulnerability to Apple because it did not purchase the rights to the technical details about the extent of the vulnerability or the method used to exploit the vulnerability.[48] The FBI subsequently told Apple about a different flaw in software running on older versions of iPhones and Macs—a flaw that Apple reportedly had already patched in an update to its operating systems.[49]

Vulnerabilities Equities Process: Administration Policy, Not Law

The Obama Administration established a process—known as the Vulnerabilities Equities Process (VEP)—to help decide whether or not to disclose information about a vulnerability that the government has discovered or otherwise obtained. The VEP was first set into motion through a

(...continued)

2014.

[43] Andy Greenberg, "Tor Says Feds Paid Carnegie Mellon $1M to Help Unmask Users," *Wired*, November 11, 2015.

[44] See In re Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. 15-0451, at 1-2 (C.D. Cal. February 16, 2016).

[45] For more information about this case and related legal and policy debates, see CRS Report R44396, *Court-Ordered Access to Smart Phones: In Brief*; and CRS Report R44407, *Encryption: Selected Legal Issues*.

[46] Ellen Nakashima, "FBI Paid Professional Hackers One-Time Fee to Crack San Bernardino iPhone," *The Washington Post*, April 12, 2016.

[47] Sayako Quinlan and Andi Wilson, *A Brief History of Law Enforcement Hacking in the United States*, New America Foundation, September 2016.

[48] Alina Selyukh, "FBI Explains Why It Won't Disclose How It Unlocked iPhone," *NPR, All Tech Considered*, April 27, 2016.

[49] Joseph Menn, "Apple Says FBI Gave it First Vulnerability Tip on April 14," *Reuters*, April 26, 2016.

presidential directive in 2008.[50] An Executive Secretariat, run by the White House's National Security Council, oversees the VEP.[51]

VEP Procedure

The VEP is triggered whenever a federal government entity,[52] including law enforcement, discovers a new hardware or software vulnerability. The VEP specifies that the entity classify and/or designate the vulnerability for special handling. The vulnerability is then formally entered into the VEP if it is both *newly discovered* and *not publicly known*.[53]

When the vulnerability enters the VEP, the Executive Secretariat notifies the points of contact for all entities participating in the VEP.[54] Any entity that determines it has equities[55] at stake will send a subject matter expert to participate in discussions about the given vulnerability. These subject matter experts then collectively submit recommendations or options to the VEP Executive Review Board. Ultimately, the Executive Review Board decides how the federal government will respond to the vulnerability. Notably, there is an appeals process if any entity with equities at stake in the vulnerability disputes the Executive Review Board's decision.[56]

VEP Decision Process

Since establishing the VEP, the government has noted that there are simultaneously benefits and challenges that arise from retaining and disclosing vulnerabilities. For instance, Michael Daniel, the former Cybersecurity Coordinator under President Obama, noted that on one hand, disclosing certain vulnerabilities may mean that officials "forego an opportunity to collect crucial intelligence that could thwart a terrorist attack[,] stop the theft of our nation's intellectual property, or even discover more dangerous vulnerabilities that are being used by hackers or other adversaries."[57] On the other hand, "[b]uilding up a huge stockpile of undisclosed vulnerabilities while leaving the Internet vulnerable and the American people unprotected would not be in our

[50] National Security Presidential Directive-54/Homeland Security Presidential Directive-23. Secretaries of State, Homeland Security, and Defense, as well as the Attorney General and Director of National Intelligence, were tasked with developing a plan for coordinating the federal government's "offensive [cyber] capabilities to defend U.S. information systems."

[51] It was previously housed within the National Security Agency.

[52] This includes contractors and private sector or foreign allies that disclose a vulnerability to the U.S. government.

[53] Electronic Frontier Foundation v. National Security Agency and Office of Director of National Intelligence: Vulnerabilities Equities FOIA, *Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process*, February 16, 2010. See also Electronic Privacy Information Center, *Vulnerabilities Process*, https://epic.org/privacy/cybersecurity/vep/default.html.

[54] Full information on participating entities is not publicly available. The FOIA documents on the VEP are redacted regarding process participants. It is suggested that participants may, at times, include the Departments of Justice, Homeland Security, State, Treasury, Commerce, and Energy, as well as the Office of the Director of National Intelligence.

[55] These may be defensive, offensive, and/or law enforcement-related reasons for wanting to retain or disclose a vulnerability.

[56] Electronic Frontier Foundation v. National Security Agency and Office of Director of National Intelligence: Vulnerabilities Equities FOIA, *Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process*, February 16, 2010. See also Electronic Privacy Information Center, *Vulnerabilities Process*, https://epic.org/privacy/cybersecurity/vep/default.html. The FOIA documents on the VEP are redacted regarding information on the appeals process.

[57] Michael Daniel, *Heartbleed: Understanding When We Disclose Cyber Vulnerabilities*, White House, April 28, 2014.

national security interest."[58] Daniel outlined a number of factors considered when determining whether the government will retain or disclose a vulnerability:

> 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?
>
> Does the vulnerability, if left unpatched, impose significant risk?
>
> How much harm could an adversary nation or criminal group do with knowledge of this vulnerability?
>
> How likely is it that we would know if someone else was exploiting it?
>
> How badly do we need the intelligence we think we can get from exploiting the vulnerability?
>
> Are there other ways we can get it?
>
> Could we utilize the vulnerability for a short period of time before we disclose it?
>
> How likely is it that someone else will discover the vulnerability?
>
> Can the vulnerability be patched or otherwise mitigated?[59]

In 2014, President Obama noted that the government should generally reveal vulnerabilities so that they can be patched rather than preserving them for use, except in situations with "a clear national security or law enforcement need."[60] It is unclear whether the Trump Administration will take a similar position on erring toward vulnerability disclosure rather than retention.

Retaining and Disclosing Vulnerabilities: Data

While the federal government has outlined a process that can be used for deciding whether or not to disclose a vulnerability, it has not provided clear data on how often this process is used and how many vulnerabilities it may retain at any given moment. In 2015, the National Security Agency (NSA) noted that "[h]istorically, the NSA has released more than 91 percent of vulnerabilities discovered in products that have gone through [its] internal review process and that are made or used in the United States."[61] The NSA further noted that the remaining 9% of vulnerabilities it did not disclose were either patched by the relevant vendors or retained for national security purposes. The discussion has not included information on the total number of vulnerabilities uncovered and does not provide a reference for the total number of vulnerabilities disclosed through the process. Of note, the NSA used an internal review process prior to the establishment of the interagency VEP, so it is not clear whether use of the VEP has resulted in a similar proportion of newly discovered vulnerabilities being disclosed.[62] It is also unclear whether federal law enforcement would disclose vulnerabilities at a rate similar to the NSA if it had its own process for vetting vulnerabilities to be retained or disclosed. Due to the nature of its investigations, law enforcement may be poised to exploit categorically different types of vulnerabilities than its foreign intelligence counterparts.[63]

---

[58] Ibid.

[59] Ibid.

[60] David Sanger, "Obama Lets N.S.A. Exploit Some Internet Flaws, Officials Say," *The New York Times*, April 12, 2014.

[61] National Security Agency, *Discovering IT Problems, Developing Solutions, Sharing Expertise*, October 30, 2015.

[62] Ibid.

[63] For instance, some have suggested hardware vulnerabilities may better serve national security purposes than law enforcement investigations. See, for instance, Steven M. Bellovin, Matt Blaze, and Sandy Clark, et al., "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet," *Northwestern Journal of Technology and*
(continued...)

RAND researchers analyzed a dataset of more than 200 zero-day software exploits that it received from a vulnerability research group.[64] RAND considers these data to be a proxy for the vulnerabilities that a "private use group" (e.g., government, defense contractor, exploit developer, or vulnerability researcher) may have.[65] Looking at the stockpile of zero-day vulnerabilities, RAND's findings indicate that about 5.7% of them will have been discovered by an outside entity after a year. If these findings can be applied to other vulnerability stockpiles, one might extrapolate, for instance, that if the U.S. government has a similar stockpile of vulnerabilities, a similar proportion of them may be discovered by an outside group—including another nation state—after a year.

RAND also determined that the average lifespan of a given vulnerability in its dataset was 6.9 years before it was patched or became publicly disclosed. In addition, 25% of the vulnerabilities only survived 1.5 years or less, while at the top end, 25% survived at least 9.5 years before being patched or publicly disclosed.[66] As such, if these findings may be reliably applied to other vulnerabilities, law enforcement or another government entity may be able to retain or exploit a given vulnerability for about 9.5 years before it is patched or publicly disclosed. Of course, this lifespan may be influenced by factors such as the desirability—by researchers, nation states, criminals, or others—of finding a specific vulnerability.

Using Known Vulnerabilities

The debate surrounding law enforcement use and disclosure of vulnerabilities generally circles around the exploitation of zero-day, or unknown and unpatched, vulnerabilities. However, law enforcement also relies upon *known* vulnerabilities to obtain certain information and evidence.[67] These known vulnerabilities may be unpatched by software vendors. Additionally, the vulnerabilities may be patched by software vendors but users may continue to rely on outdated, unpatched versions of the technology. Some experts have suggested that a majority of hacking incidents involve such known vulnerabilities, and potentially "3/4 of hacking incidents occur through means that we know about and therefore have the opportunity to fix."[68]

In some instances, Congress has mandated that certain vulnerabilities exist such that law enforcement may legally exploit these security flaws to obtain information. For instance, the 1990s brought "concerns that emerging technologies such as digital and wireless communications were making it increasingly difficult for law enforcement agencies to execute authorized surveillance."[69] Congress passed the Communications Assistance for Law Enforcement Act

(...continued)

Intellectual Property, vol. 12, no. 1 (2014).

[64] Lillian Ablon and Andy Bogart, *Zero Days, Thousands of Nights: The Life and Time of Zero-Day Vulnerabilities and Their Exploits*, RAND, 2017. Some of the researchers from this unnamed group have reportedly worked for nation states, and some of this research group's products are used by nation states. RAND notes that the data span 2002-2016.

[65] Ibid., p. 11.

[66] Ibid., p. 33.

[67] Information on known vulnerabilities may be obtained from a number of resources. For instance, information on publicly known cybersecurity vulnerabilities is contained in the Common Vulnerabilities and Exposures (CVE) database. More information is available at https://cve.mitre.org/about/. CVE is sponsored by the U.S. Computer Emergency Readiness Team (US-CERT) within the Department of Homeland Security. Additionally, the National Vulnerabilities Database (NVD) is based on the CVE list and provides additional analysis of the known vulnerabilities. For more information, see https://nvd.nist.gov/general/faq.

[68] Michael Sulmeyer and Kate Miller, "Indicting Hackers and Known Vulnerabilities," *Lawfare*, May 27, 2016.

[69] Federal Communications Commission, Communications Assistance for Law Enforcement Act, January 8, 2013.

(CALEA; P.L. 103-414) to help law enforcement maintain its ability to execute authorized electronic surveillance in a changing technology environment. Among other things, CALEA requires that telecommunications carriers assist law enforcement in intercepting electronic communications for which it has a valid legal order to carry out. Specifically, CALEA places capability requirements on telecommunications carriers mandating, among other things, that their system designs allow law enforcement to intercept wire and electronic communications and access call-identifying information.[70] Essentially, the systems must be sufficiently unsecured such that content and call-identifying information can, given a lawful court order, be accessed by or provided to law enforcement.

There have been debates around expanding the range of built-in vulnerabilities that law enforcement may utilize. For instance, Congress has debated whether to require technology companies to build back door access points into encryption such that law enforcement, when presenting a lawful warrant, may access encrypted communications or stored data. This has been one of the most contentious points of debate in the larger policy discussion on the challenges that law enforcement may encounter from evolving technology. For more information on this issue, see the following text box.

Going Dark[71]

Changing technology presents opportunities and challenges for U.S. law enforcement. While some feel that law enforcement now has more information available to it than ever before, others contend that law enforcement is "going dark" as its investigative capabilities are outpaced by the speed of technological change.[72] As such, law enforcement cannot access certain information it otherwise may be authorized to obtain. One such technology-related hurdle for law enforcement is strong, end-to-end (or what law enforcement has sometimes called "warrant-proof") encryption.[73] Other factors influencing law enforcement's ability to obtain information, and thus contributing to the going dark debate, include provider limits on data retention; bounds on companies' technological capabilities to produce specific data points for law enforcement; tools facilitating anonymity online; and a landscape of mixed wireless, cellular, and other networks through which individuals and information are constantly passing.[74]

The going dark debate originally focused on data in motion, or law enforcement's ability to intercept real-time communications. However, as communications technologies have evolved, so has the rhetoric on going dark. More recent technology changes have potentially impacted law enforcement capabilities to access not only communications but stored content, or data at rest. In this debate, administration officials and policymakers have discussed whether to require technology companies to build back door access points into encryption. Rather than pushing for loosened encryption standards, however, there has been more momentum for backing strong encryption and simultaneously supporting law enforcement efforts to bolster its technological capabilities to gain access to encrypted devices and communications.[75]

[70] 42 U.S.C. §1002(a).

[71] For more information, see CRS Report R44481, *Encryption and the "Going Dark" Debate*.

[72] See Peter Swire and Kenesa Ahmad, "'Going Dark' Versus a 'Golden Age for Surveillance'," Center for Democracy and Technology, November 28, 2011, and Federal Bureau of Investigation, *Going Dark*, https://www.fbi.gov/services/operational-technology/going-dark.

[73] See, for example, International Association of Chiefs of Police, *Data, Privacy, and Public Safety: A Law Enforcement Perspective on the Challenges of Gathering Electronic Evidence*, November 2015. See also testimony before U.S. Congress, House Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, *Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives*, 114th Cong., 2nd sess., April 19, 2016.

[74] Ibid.

[75] See, for example, testimony by Susan Landau before U.S. Congress, House Committee on the Judiciary, *The Encryption Tightrope: Balancing Americans' Security and Privacy*, 114th Cong., 2nd sess., March 1, 2016. See also House Judiciary Committee and House Energy and Commerce Committee, Encryption Working Group, *Encryption Working Group Year-End Report*, December 20, 2016.

Officials and policymakers have largely moved away from the idea of introducing what could be exploitable vulnerabilities into technology. To date, research has not demonstrated that granting exceptional access—a means by which a vulnerability could be introduced and only accessed by legitimate, authorized actors—could be controlled such that only these authorized actors (e.g., law enforcement) may take advantage of it. One group of computer scientists and security experts, for instance, contends that providing for exceptional access "will open doors through which criminals and malicious nation-states can attack the very individuals law enforcement seeks to defend."[76]

Data Issues

The discussion on whether law enforcement should generally retain or disclose zero-day vulnerabilities that it discovers/obtains lacks a number of data points that may help inform this conversation, as well as other conversations on law enforcement's relationship with technology.

One primary question centers on the effectiveness of using, or exploiting, vulnerabilities. How "effective" are these NITs, or vulnerability exploits, in developing law enforcement cases? There are a number of arguments for and against why law enforcement should retain knowledge of vulnerabilities and, if available, their exploits. However, quantitative analysis of related questions is lacking.

- In what number—and proportion—of cases does law enforcement rely on technology vulnerabilities to obtain evidence?
- In cases involving evidence obtained through the use of NITs, was this evidence more crucial than other case evidence (not obtained through an NIT) to the investigation or prosecution?
- Are there tools other than NITs that law enforcement can use to obtain the same evidence, and how often are those tools utilized?
- How often do investigators decline to pursue a suspect or case because they cannot access communications or a device and do not have an exploit (and related vulnerability)?
- What is the financial cost of developing or purchasing vulnerability exploits?
- Once a vulnerability is discovered and an exploit is developed, how many times might a given exploit be used?
- What is the impact on "innocent bystanders"? Are NITs deployed narrowly enough to avoid implicating innocent individuals?
- Are the warrants authorizing use of NITs written narrowly enough to prevent innocent individuals from having their machines and information compromised?[77]
- Can NITs introduce unintended weaknesses into the target machines/servers? Can they (and how often do they) unintentionally collect information beyond the scope of the intended target information?

[76] Harold Abelson, Ross Anderson, and Steven M. Bellovin, et al., *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, Massachusetts Institute of Technology, July 6, 2015, pp. 24-25.

[77] Ellen Nakashima, "This is How the Government is Catching People Who Use Child Porn Sites," *The Washington Post*, January 21, 2016.

Policy Issues

Lawful Hacking Intertwined with the Going Dark Debate

Within the broader going dark debate, "lawful hacking is often posited as an alternative to encryption regulation."[78] Some experts have suggested that the U.S. government should continue to support strengthening encryption and simultaneously give law enforcement resources to bolster their capabilities to conduct investigations in an environment of evolving technology and strong encryption.[79] Some have also noted that "if the executive branch is unable to successfully develop lawful hacking tools to address a sufficient amount of the need for government access to communications to meet the expectations of the general public, it becomes dramatically more likely that it will feel compelled to seek comprehensive legislative solutions mandating exceptional access."[80] These hacking tools may include exploits for both publicly known and zero-day vulnerabilities.

The ability of law enforcement to take advantage of publicly known vulnerabilities may drive the conversation on going dark. If law enforcement is readily able to exploit these vulnerabilities, the question of whether it is going dark becomes less relevant. However, if law enforcement cannot take advantage of known vulnerabilities (for whatever reason), the question remains of whether it is being outpaced by the speed and strength of technology.

Law enforcement's use of zero-day vulnerabilities (those that it would submit to the vulnerabilities equities process), however, is a different issue. One question is whether the VEP, or any potential changes to the process, could affect law enforcement's reported going dark challenges. If the VEP generally results in disclosure of vulnerabilities, law enforcement might have a more limited timeframe in which it may develop exploits for, and take advantage of, a given vulnerability. On the other hand, if disclosure results in vendors patching these holes, malicious actors may be less likely to detect and exploit the vulnerabilities.

Law Enforcement Acquisition of Vulnerability Exploits

Law enforcement may acquire knowledge of vulnerabilities through a number of means; this information may be publicly available (such as that included in the National Vulnerability Database), obtained from a hacker or vulnerabilities marketplace, or discovered. Law enforcement may obtain exploits to take advantage of these vulnerabilities by purchasing them off-the-shelf (which may not be useful to law enforcement who need to customize them for legal use), including from an online marketplace. They may also develop exploits (or contract an outside entity to develop them) tailored to suit specific law enforcement needs.

Yet another unknown regarding the acquisition of zero-day vulnerabilities or exploits is whether other entities have or will discover the same vulnerability. As former White House cybersecurity coordinator Howard Schmidt noted, "[i]t's pretty naive to believe that with a newly discovered zero-day, you are the only one in the world that's discovered it ... [w]hether it's another

[78] Susan Hennessey and Nicholas Weaver, "A Judicial Framework for Evaluating Network Investigative Techniques," *Lawfare*, July 28, 2016.

[79] See, for example, testimony by Susan Landau before U.S. Congress, House Committee on the Judiciary, *The Encryption Tightrope: Balancing Americans' Security and Privacy*, 114th Cong., 2nd sess., March 1, 2016.

[80] Susan Hennessey, *Lawful Hacking and the Case for a Strategic Approach to 'Going Dark',* Brookings, October 7, 2016.

government, a researcher or someone else who sells exploits, you may have it by yourself for a few hours or a few days, but you sure are not going to have it alone for long."[81]

Acquiring the knowledge of vulnerabilities and their exploits can be costly. Some have suggested that the knowledge of vulnerabilities and their exploits can go for upwards of $1 million on the black or grey markets.[82] RAND reports that the federal government may, however, spend more money assessing products for vulnerabilities and subscribing to vulnerability feeds[83] than it spends on purchasing zero-day vulnerabilities and their exploits.[84] If this is indeed the case, the latter choice could be more cost-effective for federal law enforcement, which operates within specific fiscal constraints. There has been speculation surrounding how much the FBI paid a company for the exploit to help obtain data from the phone of one of the shooters in the 2015 San Bernardino terrorist attack. Some have placed the price tag near $1 million.[85] It is unclear how often federal law enforcement purchases information on vulnerabilities or their exploits, how much the average payment may be, or whether the acquired material can be applied to multiple investigations. Policymakers may explore federal law enforcement budgets for acquiring vulnerability knowledge and tools to exploit these holes.

Bug Bounties

Given that there will always be vulnerabilities, some may question whether there should be more attention given to *preventing* exploits of these vulnerabilities by strengthening security rather than to *responding* to exploits and deciding how to handle them. FBI Director Comey has noted that the government needs "to be more predictive, less reactive" and that this involves, in part, a focus on reducing vulnerabilities; the public and private sectors can use information on malicious actors and their techniques to strengthen potential targets and prevent cyber incidents.[86] Some have suggested that "the U.S. government should create incentives for individuals, companies, and governments to find software vulnerabilities, publicize, and patch them, and thus reduce the risk of attack."[87] Part of this may involve establishing or promoting "bug bounty" programs.

The concept of a bounty has long been used by law enforcement (and others) to obtain leads in identifying and locating suspects in crimes. For instance, the FBI runs a Most Wanted program, offering monetary rewards for information that leads to the identification or arrest of a suspect.[88] Federal law enforcement could formalize a bug bounty program leading to information on vulnerabilities and their exploits. While this practice already occurs on an ad hoc basis, policymakers may debate whether a formalized process would be cost effective or fruitful.

[81] Joseph Menn, "Special Report - U.S. Cyberwar Strategy Stokes Fear of Blowback," *Reuters*, May 10, 2013.

[82] See, for example, Lillian Ablon, Martin C. Libicki, and Andrea A. Golay, *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*, RAND, 2014.

[83] This involves subscribing to an entity that provides updated information on zero-day vulnerabilities that have not yet been publicly disclosed.

[84] Lillian Ablon and Andy Bogart, *Zero Days, Thousands of Nights: The Life and Time of Zero-Day Vulnerabilities and Their Exploits*, RAND, 2017. See also Lorenzo Franceschi-Bicchierai, "Inside the Foggy, Shady Market for Zero-Day Bugs," *Motherboard*, October 26, 2016.

[85] Mark Hosenball, "FBI Paid Under $1 Million to Unlock San Bernardino iPhone: Sources," *Reuters*, May 4, 2016.

[86] Federal Bureau of Investigation, "The FBI's Approach to the Cyber Threat," Remarks by FBI Director Comey at the Symantec Government Symposium, August 30, 2016.

[87] Adam Segal, "Using Incentives to Shape the Zero-Day Market," *Council on Foreign Relations*, September 2016.

[88] For more information, see https://www.fbi.gov/wanted.

A number of companies have established internal bug bounty programs such that they can identify software vulnerabilities and patch them quickly. For example, Apple offers up to $200,000 for the identification of certain vulnerabilities, and this reward has been identified as one of the highest.[89] Rewards such as these may incentivize some hackers to bring vulnerability knowledge directly to vendors or affected companies rather than to law enforcement. Bug bounty programs are also familiar to the federal government, as some agencies have already piloted them for their own systems. In April 2016, the Department of Defense (DOD) launched the "Hack the Pentagon" pilot program where "hackers were provided legal consent to perform specific hacking techniques against [DOD] websites, receiving financial awards for successfully submitting vulnerability reports."[90]

While the federal government may expand its own bug bounty programs, another option that policymakers may consider is financially supporting private sector bug bounty programs through federal grants. There are a number of avenues through which various departments and agencies could provide assistance, and DOJ grants are one such angle. For one, DOJ could provide grants to support bug bounty programs at entities that share information on vulnerabilities with law enforcement. However, the success of such an initiative may be bounded by financial capabilities, as the federal government could have trouble competing with the high bug bounty rewards offered by the private sector. Grants could also be used to help entities establish internal bug bounty programs so that they would be better prepared to counter the efforts of hackers, criminals, and other malicious actors.

Sharing Vulnerabilities Information

With respect to vulnerabilities, two types of information sharing may be of particular interest to law enforcement. One involves sharing information with technology companies and the public, the other involves sharing information amongst law enforcement entities.

The Vulnerabilities Equities Process (VEP), outlined above, is a primary means by which law enforcement may share information on zero-day vulnerabilities with the technology industry and public. In examining the VEP, policymakers may evaluate whether this is the most appropriate path by which law enforcement disseminates knowledge of previously unknown and unpatched vulnerabilities.

Relatedly, policymakers may examine the issue of law enforcement disclosing details about NITs used to exploit vulnerabilities. There is no formalized or mandated process by which these tools may be evaluated for potential sharing. Law enforcement may view these details as sensitive and may even classify the tools used. Take, for instance, cases involving the Playpen website and the FBI's NIT that leveraged a vulnerability to help obtain identifying information of potential perpetrators. Even when requested in court, the FBI has declined to reveal the details of the NIT used against the Playpen website,[91] and in at least one case has opted to dismiss charges rather than reveal detailed NIT source code.[92] In addition, the FBI has classified elements of the NIT,[93]

[89] Lily Hay Newman, "Apple's Finally Offering Bug Bounties—With the Highest Rewards Ever," *Wired*, August 4, 2016.

[90] Department of Defense, *"Hack the Pentagon" Fact Sheet*, June 17, 2016. DOD has since awarded additional contracts for follow-up initiatives. See Department of Defense, "DoD Announces 'Hack the Pentagon' Follow-Up Initiative," press release, October 20, 2016.

[91] Tim Cushing, "Judge Says the FBI Can Keep Its Hacking Tool Secret, But Not the Evidence Obtained With It," *techdirt*, May 27, 2016.

[92] See Government's Unopposed Motion to Dismiss Indictment Without Prejudice, *United States of America v. Jay* (continued...)

which impedes criminal discovery—and thus potential public disclosure—of the specific NIT source code.[94] Some have questioned whether revealing details about an NIT would provide insight into *how* law enforcement is utilizing it and whether—if a court has authorized a warrant for the use of an NIT—law enforcement has acted within the authorized scope of the warrant. Others have argued that details about an NIT would reveal information about the presence of a particular software vulnerability and how the NIT was deployed to a target computer.[95] Policymakers may examine which entities should determine if and how NIT details should be revealed. Should this be decided by law enforcement, the courts, or Congress?

In sharing information on vulnerabilities and potential exploits with the larger law enforcement community, law enforcement may turn to the National Domestic Communications Assistance Center (NDCAC).[96] The NDCAC, which opened in 2013, is led by the FBI and aimed at technical knowledge management and information sharing on technical solutions between federal, state, and local law enforcement agencies. Specifically, its four core functions are law enforcement coordination, industry relations, technology sharing, and CALEA implementation. The NDCAC may be an appropriate venue for law enforcement to share information on vulnerabilities and potential exploits that may be used to leverage these vulnerabilities. In the 114th Congress, the Encryption Working Group recommended that Congress officially authorize and modernize the NDCAC to help bolster law enforcement's technical expertise.[97]

Author Contact Information

Kristin Finklea
Specialist in Domestic Security
kfinklea@crs.loc.gov, 7-6259

(...continued)

Michaud, (United States District Court for the Western District of Washington at Tacoma 2017).

[93] See Government's Response to Defendant's Motion to Compel, *United States of America v. Gerald Andrew Darby*, 22 (United States District Court for the Eastern District of Virginia 2016).

[94] Cyrus Farivar, "To Keep Tor Hack Source Code Secret, DOJ Dismisses Child Porn Case," *ArsTechnica*, March 5, 2017.

[95] See, for example, Declaration of FBI Special Agent Daniel Alfin in Support of Government's Motion for Reconsideration, *United States of America v. Jay Michaud*, (U.S. District Court for the Western District of Washington at Tacoma).

[96] For more information on the NDCAC, see http://www.ndcac.cjis.gov/about.htm.

[97] House Judiciary Committee and House Energy and Commerce Committee, Encryption Working Group, *Encryption Working Group Year-End Report*, December 20, 2016.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu