June 2017 | Sven Herpig

Government Hacking: Computer Security vs. Investigative Powers

A comparative problem analysis supported by the Transatlantic Cyber Forum

Stiftung
Neue
Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Executive Summary

Die vorliegende Analyse beschäftigt sich mit dem Spannungsfeld von IT-Sicherheit und staatlichen Befugnissen des Zugriffs auf Daten von Verdächtigen durch Hacking. Als Basis dienen die zwei Fallstudien “Operation Pacifier” (USA) und “Telegram-Hack” (DEU). Zentrale Elemente der Analyse sind das staatliche Management von Schwachstellen in Hard- und Software und die Gewinnung und Handhabung von digitalen Beweismitteln.

Die zugrundeliegende Hypothese ist, dass Deutschland und die Vereinigten Staaten die Diskussion über die Schwächung von Verschlüsselung oder mandatierte Hintertüren beenden sollten. Der Fokus sollte auf der weiterführenden Analyse alternativer Methoden zur Erlangung digitaler Beweismittel, inklusive staatlichem Hacking, liegen. Als Ergebnis formen daher folgende Aspekte die Ausgangsbasis für die Handlungsoptionen, welche die Arbeitsgruppe zukünftig erarbeiten wird:

1. Bewertung von staatlichem Hacking und Identifikation von Alternativen;
2. Evaluierung und Design eines umfassenden Schwachstellenmanagement-Systems;
3. Diskurs über die zukünftigen Herausforderungen digitaler Beweismittel;
4. Betrachtung der Angemessenheit gerichtlicher Überprüfungen;
5. Handhabung möglicher außenpolitischer Implikationen.

The analysis focuses on the discrepancy of computer security and investigatory powers when it comes to government hacking. “Operation Pacifier” (US) and the “Telegram-Hack” (GER) are the two case studies forming the basis of this research. Core elements of the analysis are governmental management of hard- and software vulnerabilities as well as the collection and handling of digital evidence.

The working hypothesis is that Germany and the United States should forego any further encryption policy and mandatory backdoors discussion and rather focus on the analysis of obtaining digital evidence through a variety of other means including government hacking. The case studies reveal that government hacking faces many challenges and comes in different shapes. The working group will focus in analysis and the development of recommendations in the following areas:

1. assessing government hacking and identifying alternatives;
2. evaluating and designing a comprehensive vulnerability management scheme;
3. discussing future challenges arising from digital evidence;
4. exploring the adequacy of judicial review;
5. mitigating possible foreign policy implications.

Contributions

Contributions to this paper have been provided by the members of the Transatlantic Cyber Forum (TCF) working group on “encryption policy & lawful hacking”. These include amongst others Cathleen Berger (Mozilla, contribution in personal capacity), Joseph Lorenzo Hall (Center for Democracy & Technology), Ernst Härtl (Digital 4TRESS), Stefan Heumann (Stiftung Neue Verantwortung), Andreas Kuehn (Cyberspace Cooperation, EastWest Institute), Julia Schuetze, (Stiftung Neue Verantwortung), Ben Scott (New America/ Stiftung Neue Verantwortung).

Introduction

Law enforcement agencies (LEAs) around the world have been alerting politicians about the serious challenge that 'going dark' (the expanded use of encrypted communication tools and the increasing complexity of the digital sphere) poses to criminal investigation and counter-terrorism operations. LEA's inability to access or read criminal and terrorist communication and stored information (data in transit and data at rest) is claimed to put public security in peril. Therefore, during the past decades, LEAs repeatedly challenged encryption policies in Germany and the United States[1].

They seek access encrypted information, for example by mandating backdoors, key escrow mechanisms or regulating encryption itself. The counter argument is clear: encryption is at the core of information security and therefore essential for all kinds of communication and information. Threatening encryption directly would endanger business models and commercial interests, weaken secure government communication as well as expose society to the risks of cyber crime even more. As a result, LEAs and the intelligence community (IC) have failed to make a compelling case for encryption regulation. So far, they have lost the 'crypto wars'[2] on both sides of the Atlantic.

Innovation and development without encryption restrictions enabled the evolution of an ecosystem featuring low cost secure communication and data storage software tools. The implementation and adoption rate of those tools spiked after the Snowden revelations in 2013, leading to a greater challenge for the LEAs[3]. As a result, agencies sought new instruments to counter 'going dark' - in particular building LEA capacity for 'government hacking'. The discussion is somewhat underdeveloped because some LEAs declined to ask for resources or propose government hacking as an alternative to mandatory decryption. One reason for this might be that they would not want to appear weakening one of their central arguments, which is: backdoors are the only answer to 'going dark'.

[1] Case studies on Germany's and United States' legal frameworks and backgrounds for government hacking http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU%282017%29583137_EN.pdf

[2] https://www.newamerica.org/cybersecurity-initiative/policy-papers/doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/ and https://www.lawfareblog.com/germanys-crypto-past-and-hacking-future

[3] However, lack of human resources in general is perceived as a much larger challenge in Germany. The German police force accumulated 22 million hours of overtime in 2016 alone: https://www.tagesschau.de/inland/polizei-183.html

The Vulnerabilities Equities Process (VEP) in the US constitutes an interagency process to evaluate the (non-)disclosure of vulnerabilities[4]. Germany on the other side recently established a Central Authority for Information Technology in the Security Sphere (ZITiS) which is inter alia tasked with acquiring vulnerabilities for security agencies[5]. While the VEP is a formalized vulnerability evaluation process with a low degree of institutionalization, Germany has created an entire agency[6] devoted to handle this vulnerability management and explore related areas, such as the procurement of government hacking tools. To serve its function, ZITiS would need a VEP-like process which is - as far as we know - currently not integrated. So far, ZITiS will only work with agencies under the Federal Ministry of the Interior, thereby deliberately excluding the military intelligence (MAD) and foreign intelligence service (BND). Caveat: ZITiS forms a colocation with the cyber defense research center of the military (CODE) in Munich. While ZITiS could learn from VEP's experience, the German setup might in turn also serve as best practice for centralized vulnerability management and provision of government hacking tools.

[4] VEP was introduced in 2009 and until 2013 headed by an executive secretariat within the NSA. After the Snowden revelations, the process was restructured and the National Security Council was tasked with overseeing the VEP. The process requires every involved agency to submit information about a newly found and publicly unknown vulnerability (0-day) to the secretariat. The secretariat then coordinates an elaborate interagency process leading to a decision about how the USG should handle the vulnerability: disclosure or nondisclosure. Most publicly available information was requested by EFF through FOIA and can be found here: https://www.eff.org/files/2016/01/18/37-3_vep_2016.pdf. VEP has been widely criticized as ineffective but just has just recently been reinvigorated by a bipartisan bill - the PATCH Act - that aims at codifying a formal statutory scheme for vulnerability management, which might replace the VEP: https://www.schatz.senate.gov/imo/media/doc/BAG17434_FINAL%20PATCH.pdf Suggestions for how to reform the VEP were already discussed before, for example in June 2016 by Schwartz and Knake, http://www.belfercenter.org/sites/default/files/legacy/files/vulnerability-disclosure-web-final3.pdf

[5] ZITiS is tasked to service security and intelligence agencies with tools and capacities for government hacking, interception and analysis. It is solely tasked to provide assistance and not engage in operational activities or pool human resources from the existing security and intelligence offices. In a first step, ZITiS will provide its services to the Office for the Protection of the Constitution (domestic intelligence) as well as to the Federal Police and Federal Office of Criminal Investigation. Further down the road ZITiS is supposed to offer assistance to additional security and intelligence agencies including those on state level, https://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2017/01/zitis-vorstellung.html

[6] ZITiS was announced in January 2017 and is supposed to be staffed with 120 employees until end of the year. As of June 2017, there are only 8 people working there, https://www.golem.de/news/verschluesselung-zitis-hat-erst-acht-mitarbeiter-und-sucht-nach-einem-auftrag-1706-128271.html

This paper seeks to interrogate thoroughly the questions raised by government hacking as a policy and practical proposal. To determine the viability and diversity of government hacking as a rational, proportionate and effective tool as compared to alternative methods to gather (digital) evidence, this paper analyses two cases:

1. the Federal Bureau of Investigation's (FBI) Operation Pacifier and

2. Germany's Federal Office of Investigation's (BKA) exploit of the Telegram messenger.

Those cases have been chosen as they present the most recent high-profile LEA government hacking operations in both countries. The comparative analysis focuses on three key aspects: information security, public security and alternative tools to obtain digital evidence.

- **"Information security"** analyses how much the general state of information security - in the framework of national security[7] - was weakened by the government hacking approach.
- **"Public security[8]"** construes the significance of digital evidence that has been gathered by the LEAs through government hacking and its impact on other parties.
- **"Alternative tools to obtain digital evidence"** explores practical options and challenges for LEAs to gather digital evidence without government hacking.

What is government hacking?

For the purposes of this paper, it makes sense to establish a clear and coherent definition of the term 'government hacking' as it is used in several ways. It is also important to distinguish where the government hacking debate overlaps with the encryption debate and where it does not. Government hacking, lawful access to data, back doors and key escrow as well as the regulation (and thereby weakening) of encryption standards are part of encryption policy. Lawful access, mandatory backdoors or key escrow as well as regulation of encryption standards do however not constitute government hacking.

Government hacking is not only part of the encryption debate but also goes beyond it. It can also be applied to devices which do not use encryption but are for example protected by other security mechanisms. What government hacking refers to is the government's exploitation of existing vulnerabilities in soft- and hardware to access data in transit and data at rest or manipulate a target's device (e. g. switching on sensors or webcams). This definition

[7] Includes all national stakeholders such as private sector entities and civil society.

[8] Refers to the security created through government hacking without factoring in the disadvantages arising from the "information security" aspect.

sets it apart from lawful access[9] and encryption regulation.

A government-developed malicious software - such as a Trojan Horse - can be installed on a target's device either remotely through government hacking or through gaining physical access to the device itself. In the latter case, the government might not even need to exploit a vulnerability to install its malware or access data on the device. Knowing the passcode for example would allow LEA to access information on the device without exploiting a vulnerability.

Successful government hacking activities might rely on a vulnerability that can be exploited to gain access to data. For the scope of this paper, a vulnerability is defined as a flaw in soft- or hardware which individually or chained with others enables third parties to perform unauthorized - and possibly covert - operations on a device or against a digital account. There are two categories of vulnerabilities, those which are already known by the manufacturer (n-days/ "old days") and those unknown to it (0-days / "oh days"). The process leading from a 0-day to a n-day is referred to as disclosure. Although n-days have been disclosed to the manufacturer, they might not be fixed - and in some cases, will never be fixed[10].

Even if a vulnerability is disclosed and fixed, it does not mean that LEAs/IC cannot exploit it anymore. The user of the respective system often still has to actively trigger the update which patches the vulnerability. If the user does not do that, LEAs/IC can still exploit it. A recent study concluded that most hacking attacks in 2015 exploited n-days which had fixes readily available[11]. Especially for large companies and/ or companies with complex IT environments as well as those dealing with certified systems, prudent patching takes quite some time. Hastily patching systems might affect them and in rare cases even render them inoperable. Thus, it might take several weeks for large environments to fully be updated.

[9] Lawful access refers to legally obtained access to communication and data provided for example by Internet Service or Telecommunication Providers to LEAs. If the communication or data is encrypted and cannot be decrypted by the provider, it is not of much use for the LEAs.

[10] For example if the vulnerability is discovered after the end-of-life-cycle of the product (no 'legacy support') or if no one exists anymore who could maintain the product and fix the flaw, https://www.techopedia.com/definition/30051/end-of-life-product-eol-product

[11] http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

'Telegram-Hack'

LEA approach

In 2014, Germany's Federal Office for Criminal Investigation (BKA) hacked[12] the 'secure' Telegram messenger accounts of eight persons[13]. The users of these accounts were suspects in an ongoing criminal investigation against an extremist right wing group. This hack allowed the BKA to access the entire history of all the non-encrypted chats[14] (including media files) connected to the account as well as all new messages in real time since all messages are centrally saved on the Telegram servers. The hack used a mixture of features and flaws in the messenger and account design.

Telegram allows the user to register several devices (smartphone, tablet, laptop) to the same account[15]. Once a new device is registered to an existing account, the server will send a text message with an authentication code to the originally registered phone number. Typing the code in the new device will automatically link the device to the account. Both devices then have full access to the account, will show all (non-encrypted) messages and can be used to send messages. In this case, the LEA had a wiretapping warrant and was therefore able to enlist the support of the telecommunication provider through which the authentication text messages were routed. The respective provider diverted these messages to the BKA device, allowing them to link their device to the suspect's Telegram account without needing any further password because 2-Factor-Authentication was not enabled on most of the victims' accounts[16]. The suspect never received an unexpected authentication message[17] and was not tipped-off.

[12] There is a dispute amongst experts if that operation fell under "mandatory access to data" passively being supplied by the telecom operator. As it contains an active hacking part which needed to be conducted by the LEA, it could also fall under government hacking and would therefore not necessarily been covered by the existing laws. While it contained elements of mandatory access, the paper assumes that entire operation more likely falls under government hacking - based on the active exploit of flaws and features of the messenger. Further details: https://motherboard.vice.com/de/article/3-5-gruende-warum-der-bka-hack-gegen-telegram-illegal-ist

[13] https://netzpolitik.org/2016/bundeskriminalamt-knackt-telegram-accounts/ and https://motherboard.vice.com/de/article/bka-telegram-hack-mitarbeiter-gericht-muenchen

[14] The encrypted one-on-one chats can only be accessed from the exact device from which they were sent and received.

[15] https://telegram.org/faq

[16] https://motherboard.vice.com/de/article/bka-telegram-hack-mitarbeiter-gericht-muenchen

[17] This would have also worked without the cooperation of the telecommunication provider. An existing vulnerability in the Signaling System 7 (SS7) protocol allows to spoof phone numbers.

At this point the BKA device was mimicking the suspect's device and gave the LEA access to the account.

When the LEA registered their own copycat phone, all devices connected to the account - including the suspect's - showed a message that a new device had been added to their account. Both, the legitimate owner of the Telegram account and the BKA now had full access to the account. To avoid detection, the BKA conducted this operation in the dead of the night and immediately used a feature in the Telegram account designed to avoid detection[18]. The feature allows a user to disconnect all devices from its account. When reconnecting to the account, the message that an additional device had been added to the account is not shown anymore (another flaw).

The only noticeable aspect of the operation for the targets was that their phone was disconnected from their Telegram account. After they reconnected it, everything appeared to be normal but the LEA had almost full access to their messenger account. The only parts LEA could not access would be 'secure' one-on-one chats which applied end-to-end encryption. Luckily for the BKA, the relevant exchanges took place in group chats which could not use end-to-end encryption or one-on-one chats which were not encrypted. There is still no default encryption in one-on-one chats or encrypted group chats. The BKA even developed a lightweight tool to automate parts of this process and monitor the ongoing chat exchanges.

The suspects could have - and some have - avoided being hacked by the BKA if they had implemented an already existing security mechanism: Two-Step Authentication. If this feature is enabled the user is asked to choose a password. From then on, every login to the Telegram account from every (known and unknown) device requires a password. In this case, the LEA would have been able to setup a copycat device but not access the messages. Again, this feature was (and still is not) enabled by default.

The data obtained from this hack -- together with other pieces of evidence -- was presented to the court that eventually convicted the suspects in spring 2017. It is unknown what role the Telegram data played in the final judgement, as there was additional human intelligence (HUMINT) information from the domestic intelligence service as well as compelling evidence obtained through conventional wiretapping[19]. The latter - and not the evidence obtained in the hack - served as a basis for the indictment.

Information security

The BKA did not harm the overall state of information security for the public. All the implementation flaws and vulnerabilities that were exploited by the LEA with support of the telecommunication provider were known by several

[18] https://motherboard.vice.com/de/article/3-5-gruende-warum-der-bka-hack-gegen-telegram-illegal-ist

[19] https://motherboard.vice.com/de/article/bka-telegram-hack-mitarbeiter-gericht-muenchen

IT-security experts, which makes them n-days[20]. Even without the help of the telecommunication provider, the BKA would have been able to conduct this hack successfully with the alternative to exploit the SS7 vulnerability[21]. The only manipulation was the forced disconnect of all devices from the account. After reconnecting, the suspects could access all messages again, therefore no information was lost or destroyed by the LEA.

LEA also did not keep those flaws and vulnerabilities from the vendor. The company behind Telegram should have known about them latest by end of 2014[22] when they became public[23]. That is why security mechanisms, such as the Two-Step Authentication exist. By not enabling end-to-end encryption and Two-Step Authentication by default however, it enabled BKA and basically everyone else to exploit those flaws for a long time.

The latter point could have led a tech-savvy court or defense attorney to the conclusion that the obtained evidence from the government hack is problematic. As shown, everyone could have tampered with the suspect's Telegram account by exploiting the SS7 vulnerability, not only receiving but also sending incriminating messages. Only Telegram may be able to discern which message was indeed sent from the suspect's device and not from a mimicking device, say by another LEA, intelligence agency or hacker[24]. The company behind Telegram however was - as far as is publicly known - not actively involved in the case. The integrity of the account and all messages sent could be regarded as compromised[25].

Additionally, the 'digital chain of custody' might be questionable. As shown, the integrity of the messages that served as evidence in court could have been compromised. The messages were not end-to-end encrypted or digitally signed. They could have been tampered with by accident through the automated software tool the BKA used. They might have even been written by a third party. There is currently no requirement to digitally sign electronic evidence during collection. Consequently, questions about their integrity are legitimate. Thus, the LEA approach did not cause any damage to the state of information security but also opened the door to fundamental questions about the handling of digital evidence that may introduce (for some observers) a reasonable doubt[26].

[20] The source cannot be attributed for secrecy reasons.

[21] https://gist.github.com/CHEF-KOCH/07ad6b8d3cd3d11435cc6dffb7b33d85

[22] However, there are reasons to believe that the vendor new about the vulnerability before it became public. The source can not be attributed for secrecy reasons.

[23] https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/german-researchers-discover-a-flaw-that-could-let-anyone-listen-to-your-cell-calls-and-read-your-texts/ and http://www.ibtimes.co.uk/hackers-links-iranian-government-attempt-map-15-million-telegram-users-1573903

[24] This would have been only possible after the LEA disclosed the devices used.

[25] https://motherboard.vice.com/de/article/3-5-gruende-warum-der-bka-hack-gegen-telegram-illegal-ist

[26] Current legal opinion might vary.

Public security

When exploiting such a vulnerability, or series of flaws, it would be prudent for the BKA to inform the Federal Office for Information Security (BSI) for further evaluation. Even though the government hacking approach had little negative consequence for information security, it still had potentially significant impact on public security in Germany and for Germans abroad as well. Telegram is marketed as a secure messenger[27], but if its security features are not enabled by the user, it is (as shown here) inherently insecure.

From a public security perspective, it might have been useful for the BKA to provide other government offices with a warning and security advisory about the vulnerabilities in the usage of Telegram. Even though the flaws were known at the point when the BKA was actively exploiting them, the decision not to inform other government agencies raises potential issues of national security, certainly in theory but also in practice. Informing government offices implicates the security standards of Germans working abroad, including senior political staff, German military, diplomats and personnel in development work. Many (if not most) use personal consumer devices and software for work-related communications[28].

Withholding information about Telegram's vulnerabilities might have exposed them to serious risks involved in being wiretapped by foreign governments and criminals. It might have even been well advised to warn operators of critical infrastructures and political communications IT-infrastructures. There are no reports that the BKA alerted the BSI or that any of them issued such warnings.

The conclusion is not as far-fetched as it might sound. Two years after German LEAs exploited the Telegram flaws and - to public knowledge - did not warn anyone about it[29], attackers were able to obtain the phone numbers of 15 million Iranian Telegram users[30]. With this data, the attackers were able to target individuals and wiretap their accounts as described above. More than a dozen accounts were compromised that way, possibly jeopardizing their own and their contacts' public security. As a reminder: Germany has personnel posted to Iran in the embassy and many other German organiza-

[27] https://telegram.org/

[28] A more efficient way could be to discourage officials using their private/ unsecured electronic devices for anything sensitive. Then Secretary of State Hillary Clinton (e-mails) and Chancellor Angela Merkel (non-secured party mobile phone) showed that this task might be futile. However, secure communication devices are expensive and not available for everyone who might be targeted - including their families.

[29] There is no public knowledge about another Telegram hack conducted by the BKA - or any other German LEA - which might warrant its behavior of not alerting anyone about it.

[30] http://www.reuters.com/article/us-iran-cyber-telegram-exclusive-idUSKCN10D1AM

tions work on politically sensitive issues around the globe. There is currently no evidence that German service personnel were affected by the attack, but this example shows the scope and potential implications of LEAs exploiting flaws and vulnerabilities without worrying about the other side of the coin.

Alternatives

As described in the case itself, the LEA had some alternative tools to government hacking. They were able to obtain information through human intelligence (HUMINT) and conventional wiretapping of calls and text messages which were not connected to the government hacking. The LEA also conducted multiple search and seizures after they obtained compelling evidence outside their government hacking approach. It is unclear whether the LEA assumed that it might not be able to obtain enough conclusive evidence, or whether other reasons led it to additionally apply government hacking as it is rather unusual in Germany.

The search and seizure could and should have also included the targets' devices used for messaging. If conducted with utmost precision, it could have also given LEA the means to access Telegram and all other data on the device, similar to the operation against the Silk Road operator Ross Ulbricht[31]. The requirement is the seizure of a device in an unlocked or decrypted state with the application in question either not having 2-Factor-Authentication enabled or recently having entered the passcode. However, there are also some workarounds for locked and encrypted devices. It might be worthwhile to expand on those options.

Additionally, the suspects planned a meeting in a small shack. That meeting could have been monitored by the LEA using conventional surveillance hardware. That was not necessary anymore because the suspects were arrested before the meeting took place. Substantial evidence which led to their arrest had already been collected through wiretapping of their phone conversations.

Conclusion

The government hacking approach adopted by the BKA was quite adept. Taking advantage of a series of software flaws in Telegram allowed it to have full access to the targets' past and present communication. Moreover, it is unknown what impact the obtained information had on the law enforcement efforts. While the approach was mainly non-invasive in information security terms, it possibly had serious impact on the public security of Germans in Germany and abroad – and thereby possibly making it an issue of national security. This predicament could be solved by alerting the national cyber security agency (BSI) when the LEA receives knowledge of a certain vulnerability or flaw that could also be used against Germans.

[31] https://www.wired.com/2015/01/silk-road-trial-undercover-dhs-fbi-trap-ross-ulbricht/

There should be a centralized focal point and clear process for collecting, managing and evaluating vulnerabilities and flaws in software and hardware. That agency's responsibility would be to determine an adequate reaction to a vulnerability or flaw: non-disclosure, disclosure to the vendor or disclosure to selected target audience such as critical infrastructure operators[32]. This process needs accountability and oversight. For some stakeholders, it is reasonable to question to what extent law enforcement should exploit a vulnerability or flaw at all, or whether this method of investigation should be out of the tool box in general. The LEA's approach also shows that it used different methods and means to successfully obtain evidence. Furthermore, it should be evaluated if other methods such as the search and seizure of the smartphones would have been more beneficial to obtaining electronic evidence or whether government hacking was indeed crucial to the investigation.

Operation Pacifier

LEA approach

Pacifier was an LEA operation conducted in 2015 against the owner and users of the Hidden Services child pornography portal Playpen. This evaluation focuses only on the activities conducted against the users rather than the owner. The FBI was informed by an unknown foreign LEA that the server of the Playpen portal was located in North Carolina. They then obtained a local warrant from a federal judge according to Rule 41 then in effect[33] and seized the server. Instead of shutting down the portal, the FBI ran it from its own servers in Newington, Virginia for two weeks (February 20 – March 4)[34]. It did so to use it in a targeted operation against the portal's visitors.

The portal was only accessible through Tor's hidden services. Therefore, even by taking over the technical infrastructure completely, nothing useful – in terms of evidence – was known about the users. Exploiting a vulnerability in the Tor browser bundle, which is required to access sites like Playpen, the FBI converted the platform into a bulk delivery mechanism for its own malicious software. FBI referred to its malware as network investigative technique (NIT). Once the users accessed certain areas of the portal, their systems were automatically infected with the NIT. It then sent information

[32] Even though the Telegram flaw was known, the BSI apparently did not issue any alert to other government agencies around the time that the BKA was exploiting it. The source would like to remain anonymous.

[33] Rule 41 only pertains to devices within jurisdiction of the court that issued the warrant and the FBI had no way of knowing where the affected computers would be located. It was highly probable that the devices were not only located outside the district (which covers the portion of Virginia that includes Newington) but also outside the country. Rule 41 was amended in December 2016 to let judges issue warrants that allow LEAs to compromise systems outside the court's geographic jurisdiction.

[34] https://www.documentcloud.org/documents/3032955-Motion-to-Dismiss-Indictment-in-Chase.html

(i. a. operating system, real IP and MAC address) about the infected system back to the FBI[35].

The malware eventually used by the FBI was delivered to more than 8,000 computers in 120 countries around the world. The FBI shared information with other countries and used the evidence against Americans for a series of indictments[36]. Neither the exact exploit nor details about the malware that was used have been disclosed to the public or the responsible vendor[37]. It is unclear whether the prosecution must provide the defense counsel with the technical details used to obtain digital evidence. Apparently, it is to some degree up to the discretion of the judges whether the prosecution has to reveal this information[38].

This led to the paradoxical situation that the very same judge decided differently in two similar cases both pertaining to Operation Pacifier. In one case, federal Judge Bryan denied the defense‘s request to suppress evidence (United States v. Tippens) and in the other he granted it (United States v. Michaud)[39]. If it becomes common practice that LEAs do not have to reveal technical information (about exploits) in criminal proceedings, it will be easier for them to enlist IC assistance[40] and gain the benefit of exploits that these national security agencies would not offer if it entailed the risk of disclosure at trial. So far, the fallout from this case has been a legal debate about the one-to-many application of the search warrant pursuant Rule 41 and the – apparently even more efficient – FBI-hosting and delivery of child porn material[41].

[35] https://www.eff.org/deeplinks/2016/09/playpen-story-fbis-unprecedented-and-illegal-hacking-operation

[36] As of May 2017, the Operation Pacifier resulted in approximately 900 arrests and the rescue of nearly 300 children worldwide according to https://www.independent.co.uk/news/world/europe/europol-fbi-joint-investigation-operation-pacifier-uncovers-global-paedophilia-ring-870-arrests-a7722821.html

[37] At least until April 2016, https://motherboard.vice.com/en_us/article/the-fbi-may-be-sitting-on-a-firefox-vulnerability

[38] The analysis of whether the defense is entitled to the information will depend on whether the information is material to the defense. Depending on the defense‘s theory of the case, information might be material to the defense in one case, but not material in a different case: https://cyberlaw.stanford.edu/blog/2017/05/government-hacking-evidence-and-vulnerability-disclosure-court

[39] It is unclear why it turned out like this: https://arstechnica.com/tech-policy/2017/03/doj-drops-case-against-child-porn-suspect-rather-than-disclose-fbi-hack/

[40] One of the reasons the IC do not want to meddle with LEA cases is that they are unwilling to ‘burn’ their technical means for a criminal investigation. Those were apparently the same exact deliberations that led to the disconnection of Germany’s foreign intelligence service from the new agency ZITiS.

[41] https://motherboard.vice.com/en_us/article/doj-fbi-child-pornography-sting-playpen-court-transcripts

Information security

Evaluating the impact on the state of information security is rather difficult as there is not a lot of information available regarding the exploit and the malware used by the FBI. It is unclear but likely, given that the FBI until now has not been willing to reveal information about it, that it was a 0-day[42]. Technically speaking, it might have been an n-day as the Tor bundle only rolled out automated patches after the operation was already ongoing. At that point, only those constantly applying manual updates would have been protected against it, that is if it was an n-day exploit.

While it is likely that the vulnerability also affects the Firefox browser, it is not entirely clear if it only exists in the hardened version of the Firefox browser, which is used in the Tor bundle, or if it also exists in the regular version as well. In either case, the vulnerability has potentially massive impact on the state of information security[43]. If it exists in every Firefox version, hundreds of millions of users are at risk of being targeted by other intelligence agencies and criminals alike. If the vulnerability only exists in the Tor bundle, it is still problematic.

Tor was initially created by the U.S. Office of Naval Research and DARPA and heavily relies on USG funding (namely from the State Department). It is not only used by criminals but by people whose life depends on confidential information, such as journalists, informants, dissidents and opposition politicians in authoritarian countries as well as by companies conducting business intelligence and carrying out acts of law enforcement for research purposes. Once other parties find out about the vulnerability and begin to exploit it – maybe they have already – it gets dangerous.
This leads to two areas which should be explored further: vulnerability management and rediscovery of vulnerabilities.

Public security

Like in the German case, the question about the digital chain of custody is again a relevant one. Without knowing exactly how the NIT operates, it is impossible to say if the evidence (IP address etc.) has been (or could have been) tampered with by a third party.[44]

[42] In November 2016, security researchers found a 0-day vulnerability in the wild which carried a payload similar to the one used by the FBI in 2013 in the Freedom Hosting case. It is however unclear if the 0-day found is the same one used against Playpen users https://arstechnica.com/security/2016/11/firefox-0day-used-against-tor-users-almost-identical-to-one-fbi-used-in-2013/

[43] https://www.lawfareblog.com/hanging-internet-users-out-dry

[44] https://cyberlaw.stanford.edu/blog/2017/05/government-hacking-evidence-and-vulnerability-disclosure-court

End-to-end encryption and digital signatures are likely to play a key role in the future, and the judicial aftermath of Operation Pacifier might just be the first step. In the case United States v. Jay Michaud, the prosecution dropped all the charges because the court ordered it to reveal the method (NIT) used by the FBI to obtain the evidence. Few of the 200 cases had similar pending motions, but there were also rulings stating that the defendant was not entitled to the spyware source code – which misses the point. If the FBI would reveal the way its NIT works, Mozilla or the Tor programmers respectively would be able to fix the vulnerability and the FBI would lose its ability to conduct similar operations in the future. Government hacking does little to directly enhance public security if the obtained evidence is not allowed to be used in the courtroom. However, assessing the information might enable LEAs to explore other ways to gather admissible evidence against the suspect[45]. In that case government hacking can be viewed as a questionable means to an undeniably moral end.

It is questionable if this case of government hacking eventually contributed massively to public security. Being able to identify hundreds of child porn consumers[46] is a big win, but only if cases can actually be prosecuted in court - though certainly it helps LEAs to keep tabs on them. At the same time, public security is put at risk by not disclosing the vulnerability and thereby leaving all Tor users – and possibly Firefox users – unprotected. As mentioned above, this is a serious threat to Americans and non-Americans alike.

Alternatives

At first glance, it does not seem like there was an alternative to the FBI's approach, if they did not have any other information about the users of the platform before. The FBI could have just shut down the server and not engaged in government hacking (and hosting child pornography as a by-product). It is unclear if any of those cases would have been successfully made without that operation. The DOJ dropped cases in which it would have to reveal the source code of the NIT. This shows that the FBI might want to keep the tools in store for other, potentially "more important", cases or other currently ongoing investigations. An alternative explanation is that the exploit came from the IC and the FBI does not want to reveal its source. A direct result – one might say a political success for LEAs – was the final push[47] for the

[45] This process of recreating or gathering evidence through conventional investigative tools which is known or facilitated by otherwise dismissible means is called 'parallel construction'. It is formally prohibited but known to be exploited in the US, for example in a StingRay case of the Oklahoma City police department, https://assets.documentcloud.org/documents/2825761/OKCPDFBI-MOU.pdf

[46] According to Motherboard article "over 350 arrests, 25 child pornography producers and 51 hands-on abusers prosecuted, and 55 American children who were subjected to sexual abuse successfully identified or rescued; overseas, 870 arrests and at least 259 sexually abused children identified or rescued", https://motherboard.vice.com/en_us/article/doj-fbi-child-pornography-sting-playpen-court-transcripts

[47] https://www.regulations.gov/docket?D=USC-RULES-CR-2014-0004

amendment of Rule 41 to allow remote search and seizure in computer systems outside the federal judge's jurisdiction.

Conclusion

The FBI's approach might be sustainable but not necessarily scalable. Other LEAs, especially local ones, do not have access to 0-day exploits - hence the creation of ZITiS in the German case. It is unlikely that the FBI or IC would be willing to potentially 'burn' a 0-day exploit for a local investigation. The FBI is clinging to its exploits and allowing cases to be dropped as a direct result of it. The current approach becomes unsustainable at the point where LEAs must reveal their technical means of gathering evidence to the court and defense counsel.

Government hacking which relies on 0-days will then be reserved for high-profile cases only. Some more thought should therefore be put into alternatives, including a self-restriction to n-days instead of 0-days[48], weighing the carefully criticality of a vulnerability, but also how government hacking could be more rewarding without endangering information and public security the way this operation did[49].

Something that has not yet been portrayed in detail – because surprisingly it did not backfire so far – was the fact that the FBI indiscriminately hacked computers worldwide. Even if the targets were criminals trying to access illegal material according to American law, the possible repercussions of automated hacking of foreign computers could be immense - especially if (unknown) third parties are involved.

Problem analysis

When it comes to government hacking and weighing the equities of information security and public security, Germany and the United States face similar challenges. The greatest challenge is the 'handling' of vulnerabilities and flaws in possession of LEAs and intelligence agencies. Even though it might prove difficult to estimate the damage done to the general state of information security, the case studies, especially the American - show that

[48] Non-disclosing 0-days bears a much higher risk of national security being endangered by other stakeholders exploiting that vulnerability against government agencies or critical infrastructures. However, n-days can be as damaging if they are not addressed by those taking care of IT-infrastructures - compare WannaCry, http://money.cnn.com/2017/05/13/technology/ransomware-attack-who-got-hurt/index.html. A government restriction to n-days would at least allow those in charge of information security to have the best information available. If they use it to secure their systems in a timely manner or not is then not in the hands of the LEAs anymore.

[49] Bringing up the issues of electronic signing of evidence, tamperproof obtaining of evidence and classification of hacking tools. The FBI apparently classified its NIT to not reveal it in court while the CIA unclassified its hacking tools to be able to use them on the public Internet. The latter was revealed in the discussions surrounding Wikileaks' Vault7 revelations, https://wikileaks.org/ciav7p1/

nondisclosure can potentially have devastating impact on national security. The claim that nondisclosure does not create a direct[50] information security risk and therefore also a public security risk, only holds true as long as no malicious actor discovers the same vulnerability. The higher the rediscovery rate of a certain vulnerability is, the more likely it should be disclosed.

Another issue which is shown in the case studies and has recently been reinvigorated by Bruce Schneier[51], is the question of proportionate and effective alternatives to government hacking and backdoors/key escrow. The mentioned cases are very different in that regard. It is unknown if LEAs had other means and evidence available to substitute for government hacking in Operation Pacifier. German LEAs obviously had several options to choose from, such as the conventional wiretapping which they applied. It is worthwhile to discuss at what point government hacking is the tool of choice, the last resort or even "off limits" with regards to the damage to information security assessment.

Furthermore, it should be discussed who would make this decision (the courts, security agencies etc.) and if it is a decision made on a case by case basis or rather a set of guidelines which can be applied freely. Both operations also show that the international political dimension must be considered when government hacking is conducted targeting systems in other countries.

Lastly, the integrity of the digital chain of custody has been raised in-between the lines. Information security is said to consist of confidentiality, integrity and availability (CIA) of the information. Analyzing the two cases, it seems that integrity plays a significant role in security of digital evidence. The application of end-to-end encryption and/or digital signatures needs to be discussed as part of the government hacking strategies.

Hypothesis and further research

The working hypothesis is that Germany and the United States should forego any further encryption policy and mandatory backdoors discussion and rather focus on assessing vulnerability management and tools to obtain digital evidence through a variety of means including government hacking. Based on the problem analysis, the hypothesis leads to a five-pronged strategic approach for further research including:

1. assessing government hacking and identifying alternatives;
2. evaluating and designing a comprehensive vulnerability management scheme;
3. discussing future challenges arising from digital evidence;
4. exploring the adequacy of judicial review;
5. mitigating possible foreign policy implications.

[50] It creates an indirect threat to information security as it encourages the vulnerability black market activities.

[51] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2938033

Assessing government hacking and identifying alternatives

The case studies reveal that government hacking faces many challenges and comes in different shapes. The Telegram Hack and Operation Pacifier are two very opposite approaches. Thus, it is useful to assess various levels of government hacking and their effectiveness and proportionality as well as potential technical, organizational and legal restrictions.

Another take-away for further research concerns alternative tools for obtaining (digital) evidence. Their analysis, development and assessment needs to be strengthened. Exploring alternatives to government hacking not only benefits the LEAs by giving them more options. It might also increase overall security when LEAs rely less on their hacking capabilities. Alternative tools include amongst others traditional surveillance, search and seizure, wiretapping or GPS tracking. This discussion should also involve a take on government hacking as last resort.

Evaluating and designing a comprehensive vulnerability management scheme

The FBI Operation Pacifier highlighted the challenge that sometimes there is no alternative to government hacking. However, it also showed that government hacking requires taking into account a number of considerations. Balancing computer security and investigatory powers can be accomplished through a transparent and accountable vulnerability management scheme. The evaluation of vulnerabilities as well as the impact of disclosure or non-disclosure is vital[52].

This requires developing a metric (disclosure/retention) taking into consideration indicators, such as dissemination, potential damages and application area of the vulnerabilities in the respective hard- and software products.

At the core of the vulnerability disclosure debate is the question whether another stakeholder already has access to the same vulnerability[53].

[52] WannaCry might serve as a good case study to identify what needs to be done better, https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html and https://www.foreignaffairs.com/articles/2017-05-30/why-nsa-makes-us-more-vulnerable-cyberattacks

[53] Research undertaken in this field defines it as “collision rates” or “0-day life expectancy”. There have been two recent publications by Schneier and Herr and by RAND, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2928758 and https://www.rand.org/pubs/research_reports/RR1751.html

The Wikileaks and Shadow Brokers revelations show that a possible hack and leak of those vulnerabilities also needs to be taken into account, https://wikileaks.org/ciav7p1/ and https://medium.com/@shadowbrokerss/dont-forget-your-base-867d304a94b1

At the point where several parties have knowledge of a vulnerability, the best course of action may be to disclose the vulnerability, so that patches can be provided for it by the vendor. This however depends also on the kind of vulnerability as well as the potential impact it could have referring to the necessity of an overall vulnerability assessment.

Due to the manpower and resources it takes to tackle such a complex topic, it is reasonable to establish - or at least appoint - a central national authority dealing with all the non-operational issues concerning government hacking. That authority should not only be a 'vulnerability broker' but also explore the various non-hacking tools to obtain digital evidence and deal with future questions such as integrity of digital evidence. The authority could be designed as a service provider for national/ local LEAs as well as the IC and serve as single point of contact (interagency consultations) in this area.

Discussing future challenges arising from digital evidence

Much of evidence that LEAs and the IC will obtain in the future is digital. That kind of evidence is not only gathered through government hacking but also through other means. Handling digital evidence, no matter how it was obtained, will therefore play a significant role in the future. The US case reveals that not only the hacking itself poses questions but also the admission of digital evidence in court. In order to develop a comprehensive strategic approach to government hacking, the nature and handling of digital evidence must be factored in by design assessing digital forensics in respect to government hacking.

Exploring the adequacy of judicial review

Judicial oversight in both countries will increasingly have to deal with digital evidence obtained by LEAs through government hacking. Technical details of government hacking operations can be complex but need to be broadly understood by the presiding judge. The complexity is not limited only to the gathering and integrity of digital evidence but goes so far as the involvement of the IC and parallel construction of evidence. Operation Pacifier presents many of those (judicial) challenges.

The (to some extent) paradoxical and incoherent judicial decisions (some required disclosure of technical methods to defense counsel and some did not) further highlight this problem. It is therefore prudent to explore whether the existing rules governing wire-tapping authority and judicial review of communication 'intercepts' are sufficient or if adjustments have to be made.

Mitigating possible foreign policy implications

In Operation Pacifier, users from countries worldwide were automatically targeted and attacked. This raises security issues as it could be considered a form of espionage (or even sabotage) by the relevant country. The Telegram hack also has a foreign policy dimension as LEAs and the IC in this way set controversial precedent for less democratic countries, encouraging them to spy on their citizens. LEAs of democratic countries should consider their role model function in international relations.

Moreover, moving further in this direction, it may harm businesses operating abroad which could damage the growing transatlantic digital economy. For example, the FBI director said recently in a congressional hearing that they aim to work together with businesses to find a way to accommodate the needs of LEAs without backdoors. However, this raises the question to what extent other nationals using American services would be shielded from US LEA investigations.

About us

The **Transatlantic Cyber Forum (TCF)** has been established by the Berlin-based think tank **Stiftung Neue Verantwortung (SNV)**. The TCF was made possible by the financial support of the **Robert Bosch Stiftung** and the **William and Flora Hewlett Foundation**. The SNV is an independent think tank that develops concrete ideas as to how German politics can shape technological change in society, the economy and the state. TCF is an intersectoral network of experts from civil society, academia and private sector working in various areas of transatlantic cyber security and cyber defense policy. It currently consists of three working groups. This analysis has been conducted by the working group on encryption policy & lawful hacking which is composed of 35 experts.

Imprint

Stiftung Neue Verantwortung e. V.
Beisheim Center
Berliner Freiheit 2
10785 Berlin
T: +49 (0) 30 81 45 03 78 80

www.stiftung-nv.de
info@stiftung-nv.de
Twitter: @SNV_berlin

Design:
Make Studio
www.make-studio.net