

Government Hacking

What is it and when should it be used?



Encryption is a critical component of our day-to-day lives. For much of the world, basic aspects of life rely on encryption to function. Power systems, transport, financial markets, and baby monitors¹ are more trustworthy because of encryption. Encryption protects our most vulnerable data from criminals and terrorists, but it can also hide criminal content from governments.

Government hacking is one of the approaches national security and law enforcement agencies use to obtain access to otherwise encrypted information (e.g. the FBI hired a hacking company to unlock the iPhone at the center of the San Bernardino case²). It complements their other efforts to obtain exceptional access³ by asking or requiring tech companies to have the technical ability to decrypt users' content when it is needed for law enforcement purposes.

The Internet Society believes strong encryption is vital to the health of the Internet and is deeply concerned about any policy or action that might put that in jeopardy — regardless of its motivation. Government hacking poses a risk of collateral damage to both the Internet and its users, and as such should only ever be considered as a tool of last resort.

Government hacking defined

We define 'government hacking' as government entities (e.g. national security or law enforcement agencies or private actors on their behalf) exploiting vulnerabilities in systems, software, or hardware to gain access to information that is otherwise encrypted, or inaccessible.

Dangers of government hacking

Exploiting vulnerabilities of any kind, whether for law enforcement purposes, security testing, or any other purpose, **should not be taken lightly**. From a technical perspective, hacking an information, communications, or technology (ICT) resource without consent of the user/owner is always **an attack**, regardless of its motivation. Attacks can damage a device, system, or an active communications stream, or leave them in a less secure state. This significantly increases the risk of future breaches, potentially causing harm to all users of the system.⁴

The risks are exacerbated when governments exploit "zero-day vulnerabilities" — vulnerabilities in software or hardware that are unknown to the vendor or that have not yet been mitigated (e.g. no patch has been released).

1 Well-designed baby monitors and security cameras should be sending their data confidentially over the Internet - not all of them do.

2 https://en.wikipedia.org/wiki/FBI%E2%80%93Apple_encryption_dispute#Apple_ordered_to_assist_the_FBI

3 <https://www.internetsociety.org/wp-content/uploads/2019/05/FactSheet-EncryptionVsLawful-Access-EN.pdf>

4 Besides there is a risk that exploits may damage the integrity of digital evidence.

This approach is particularly dangerous as it exposes the Internet and its users to new security risks for which there is no ready defence. Hence, there must be coordinated disclosure of discovered security vulnerabilities as soon as possible so that they can be patched.⁵

Exploits can be stolen, leaked or replicated. Even government entities with the highest levels of security have been compromised. For example: the ShadowBrokers group hacked the U.S. National Security Agency and publicly exposed the agency's EternalBlue zero-day exploit⁶; the Italian security firm, Hacking Team, was hacked in 2015⁷; and a collection of Central Intelligence Agency hacking tools known as Vault 7 were leaked in 2017.⁸

Any exploit, regardless of its origin, can be re-purposed by criminals or nation state actors to attack innocent users. The Petya/NotPetya ransomware (based on EternalBlue) caused real-life consequences such as delays in medical treatment, suspension of banking operations, and disruption of port services.⁹ These incidents highlight the dangers of hoarding zero-day vulnerabilities and creating and storing exploits.

Commercial hacking teams do not only sell their services to the “good guys”. In 2019, security researchers discovered that the software from the NSO Group, an Israeli cyber intelligence firm used by many government agencies, had been used to covertly hack into the WhatsApp accounts of journalists and activists to surveil their communications.^{10 11}

One target can turn into many. While ideally, by design, government hacking is intended to be targeted and surgical, hacking techniques and exploits, even if intended for only one target, can also be used against a great number and variety of devices or software. Further, exploits can also be used by countries for other purposes, e.g. to engage in cyber-attacks or cyber warfare by various advanced persistent threat actors (APTs)¹² that are often state aligned. Possibly the most famous example of an APT is the Stuxnet virus, allegedly created by the U.S. and Israeli governments to destroy Iranian nuclear centrifuges, then spread around the globe (well beyond the intended target) affecting millions of other systems.¹³

Weaknesses in computer systems are discovered by attackers all the time. Keeping a weakness secret (to exploit it later) won't prevent it from being discovered by others. For example, for the Android operating system, the rediscovery rate for high and critical severity weaknesses is as much as 23% within a year.¹⁴ Given the existence of weaknesses, the most motivated — like criminals, terrorists, and hostile governments — will work harder than anyone else to find and exploit them. Their value is demonstrated by the prices and demand in black and grey markets.¹⁵ Having deployed working exploits to reverse engineer will make that even easier.

Crossing jurisdictions. There is also the risk of inadvertently infiltrating or tampering with a foreign nation's networks or systems — an act that could be regarded as an attack against the nation, its interests or its citizens, with the associated political, economic and potential cyber-attack consequences. It also may encourage some countries to pursue a sovereign Internet approach.

5 This goes further than a call to create Vulnerability Equities Processes (such as e.g. <https://cyberstability.org/norms/#toggle-id-5>) in that it calls to disclose every vulnerability.

6 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-dbb23c75d82_story.html

7 https://www.vice.com/en_us/article/3k9zzk/hacking-team-hacker-phineas-fisher-has-gotten-away-with-it

8 https://en.wikipedia.org/wiki/Vault_7

9 <https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how>

10 <https://www.nytimes.com/2019/05/13/technology/nso-group-whatsapp-spying.html>

11 <https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/>

12 <https://www.cisco.com/c/en/us/products/security/advanced-persistent-threat.html>

13 <https://www.cybereason.com/blog/advanced-persistent-threat-apt>

14 Herr & Schneier, “What You See Is What You Get: Revisions to Our Paper on Estimating Vulnerability Rediscovery”, Lawfare 2017

<https://www.belfercenter.org/sites/default/files/files/publication/Vulnerability%20Rediscovery%20%28belfer-revision%29.pdf>

15 See e.g. https://en.wikipedia.org/wiki/Cyber-arms_industry#Notable_markets for some named examples of those markets

The Internet Society's Position on Encryption and Government Hacking

As a technical foundation for trust on the Internet, encryption promotes freedom of expression, commerce, privacy, and user trust, and helps protect data and communications from bad actors. The Internet Society believes¹⁶ encryption should be the norm for Internet traffic and data storage.

Legal and technical attempts to limit the use of encryption, even if well-intentioned, will negatively impact the security of law-abiding citizens and of the Internet at large. **Government hacking to circumvent encryption** also risks the security of innocent users, critical systems (including government networks and services), and the Internet.

We do not support government hacking that poses a risk to the security of the Internet and its users. Because of the risk of collateral damage, it should never become a routine approach for law enforcement or governments to gain access to encrypted content. We also oppose laws and other rules that require tech companies to build security vulnerabilities into their products and services.

The risk is particularly acute for government hacking that relies on zero-day vulnerabilities and exploits (as noted above). However, it is also a risk even where vulnerabilities are known, but there has been minimal patching across the Internet (e.g. because equipment is too old, people cannot afford newer, more secure devices, or due to inadequate or lax patching procedures).

A main concern is that any exploit of any system creates an inherent danger. Even in a perfect scenario where a government entity uses an exploit with the best of intentions, with proper authorisation, and with a positive result; there is a high risk that the exploit will not stay within the confines of that government. The system as a whole becomes less secure merely by using the exploit, regardless of the intention.

Given the inherent risks, governments should not collect, purchase, create, store or exploit vulnerabilities for the purposes of gaining access to information for national security or other law enforcement purposes unless the following conditions apply:

- **Serious** — when it can be demonstrated that it is necessary to protect human life, counter imminent and significant risks to public safety, or prevent the most serious of crimes.
- **Last resort** — when there is no other viable alternative.
- **Judicial** — when it is pursuant to a properly executed judicial warrant.
- **Proportionate** — an operation can be objectively considered a targeted and proportionate undertaking that is scoped as narrowly as possible.
- **Risk mitigation** — there is no foreseeable risk of damage or other harm to the security of others.
- **Procedural** — an impact assessment, based on established criteria, must be completed and assessed **in advance**. The criteria should be **transparent and defined** by relevant stakeholders. This should include, but is not limited to, law enforcement, judicial officers, technical specialists, and civil society. **Each instance** of government hacking must be approved based on the pre-approved criteria.

The Internet Society urges governments to prioritise other avenues for information and evidence collection that do not present a risk to the security of devices, software, and Internet services. This includes analysis of the wealth of open source intelligence, accessible data held by service providers, relevant communications metadata, and gathering non-digital evidence such as information from witnesses and documents.

¹⁶ The Internet Society does not stand alone in this belief. For instance, the UN special rapporteur on Human Rights and the OECD have both made strong statements in support of cryptographic tools. See <https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx> and <http://www.oecd.org/sti/ieconomy/cryptography.htm> respectively.