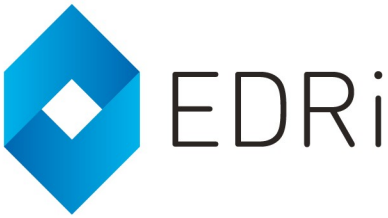

PROTECTING DIGITAL FREEDOM

Encryption Workarounds

A digital rights perspective

Final version: 12 September 2017

European Digital Rights 20 Rue Belliard, 1040 Brussels www https://edri.org twitter @edri_org tel +32 (0) 2 274 25 70

“I believe that encryption is a civic responsibility, a civic duty.”

Edward Snowden

Contents

Introduction

This brief responds to the European Commission's policy development work on encryption, in particular its consultation exercise around the Encryption Workarounds paper published by Orin Kerr and Bruce Schneier. We do not address whether or not this is an appropriate basis for such policy development.

It is important that policy decisions which can so adversely infringe upon the fundamental rights of individuals are based in evidence and have a solid justification, rather than being guided by what is politically salient - and potentially misleading. For example, it is worth recalling that the imposition of telecommunications data retention as a law enforcement tool led to the existence of an illegal EU instrument which neither the European Commission nor EU Member States were able to defend credibly in court. Ultimately, it was rejected by the Court of Justice of the European Union as a breach of the Charter of Fundamental Rights of the EU.

It is also worth noting that much of this conversation around encryption is driven by the notion that investigations, and thereby law enforcement, are "going dark" because of encryption; a premise recently questioned by Harvard's Berkman Center for Internet and Society in a report entitled 'Don't Panic'. One of the many reasons given for why the notion of "going dark" is far overblown is that even encrypted communications still generate metadata – e.g. who communicated with whom, how often, for how long, how frequently, using what network, etc. – it is often more valuable to an investigation than the encrypted content itself. Surveillance using metadata can constitute a serious privacy violation, though arguably in ignorance of this, Member State laws often are more permissive on the collection of metadata than content. Several EDRi members, Privacy International among them, have documented how damaging and overly extensive the use of metadata by law enforcement can be. However, metadata can help in key investigative tasks such as establishing the existence of networks of individuals, and in identifying locations and patterns of activity. The use of the internet has increased, and will continue to drastically increase, meaning that the amount of metadata available to law enforcement authorities will also drastically increase. This has contributed to the notion that we are in fact in a golden age of surveillance.

The heart of the Kerr / Schneier paper at issue here is that the growth in people using the internet, particularly for sensitive information and communications, has led to an increase in the development and use of strong encryption which may, in some cases, stymie law enforcement authorities. However, even in these cases there are still many workarounds available.

Each of the described methods in the paper may work in some cases but not in all, and each workaround has a unique impact on fundamental rights. For example, guessing the passphrase/password to access an encryption key is seemingly simple, but social engineering may conflict with the Charter of Fundamental Rights depending on the method used. When defining its policy, the European Commission should pay attention to the fact that the legal systems of the 28 EU Member States are very diverse and contain different, valuable safeguards for an infinite amount of challenging situations – and should note the current challenges to the rule of law in certain EU Member States.

The issue of government hacking should be examined particularly closely. Recently, we have seen several high-profile examples of governments hacking into devices or accounts for law enforcement or national security purposes by exploiting security flaws. The exploitation by GCHQ of Belgacom in order to place EU institutions under surveillance may be salient in the reader's mind. Government hacking needs to be considered from the perspective of universal human rights standards, including its interference with the rights to privacy, free expression, and due process. There has yet to be an international public conversation on the scope, impact, or human rights safeguards for government hacking. The public requires more transparency regarding government hacking – and not just about techniques, targets and volumes but also how and when hacking activity has had unanticipated impacts.

There are six workarounds discussed in the paper: find the key, guess the key, compel the key, exploit a flaw in the encryption software, access plaintext while the device is in use, and locate another plaintext copy. They can be split into two general approaches under which the first three workarounds are strategies to obtain an existing key to unlock encrypted data, and the second three are ways of bypassing the encryption altogether to access the data in plaintext form. While many of the workarounds presented in this paper raise no significant new legal questions than those that arise in more traditional settings that don't involve encryption, they do highlight and raise the stakes for situations where current law and policy

fails to provide adequate protections for fundamental rights, and their use makes reform of those laws and policies much more urgent.

Approach 1: Obtain the key

As mentioned, the following three strategies aim to obtain an existing passphrase or key to unlock encrypted data. The way these practices are accepted and used will vary greatly based on Member State national legislative frameworks, many of which could prove antithetical to one another. It is up to the Commission to navigate these nuances if it wishes to proceed with any of them. We have sought simply to shed a light on the way they would implicate the individual's' fundamental rights online.

Proposed Workaround: Find the key

There is no practical difference between carrying out a physical search for a copy of a key and searching for any other piece of evidence. The key, passphrase or password could be written on a scrap of paper, saved in a USB drive, saved on the device and accessed via a saved password (by itself or in a password manager) on a device which, itself, is not encrypted.

Therefore, such an approach does not raise any significant new legal issues from those involved in more traditional searches. Obviously, all proportionate safeguards need to be put in place and respected. Further safeguards measures should be put in place with regard to the right to access specific information on a decrypted device, not least due to the extensive and, by default, highly sensitive data that can be stored on or accessed by a device.

However, as in the example in the Kerr / Schneier paper, this can cover a range of activities from the covert installation of a keylogger on a suspect's device to the simple use of CCTV to try to identify the code being input in a public place.

Physical Surveillance

Use of CCTV and other physical surveillance does not undermine the integrity of the encryption technology itself.

While this option carries fewer consequences from a digital rights perspective, it still amounts to surveillance and should be subject to the same necessity and proportionality tests. There is a need for the European Commission and EU Member States to initiate a comprehensive review and reform of current surveillance measures and put an end to human rights violations that have crept into operational practices over time.
In 2015, the European Parliament adopted a second report on the implementation of the Habeas Corpus, examining the state of play of surveillance programmes. The report found that there has not been sufficient action to reform surveillance practices that affect individual rights. It also criticised the establishment of new surveillance measures in a large number of EU countries. The European Commission has remained silent in response to the Parliament's recommendations in the first report, which asked for urgent reform to address interferences with human rights. The Commission is failing in its duty as a Guardian of the Treaties, as it has decided not to take action in response to EU Member States' use and extension of data retention mandates and other unlawful surveillance measures.

The European Commission and European Union Member States need to initiate a comprehensive reform of current surveillance measures and put an end to human rights violations. In doing so, we recommend that governments follow their commitments under the European Convention on Human Rights, apply the Necessary and Proportionate principles, and use the implementation guide developed by EDRi member Access Now to ensure compliance with international human rights law.

Incidental copies

This can simply refer to situations where the encryption key is deliberately stored by the user's computer memory, allowing someone with access to the computer to the encrypted material, possibly without even learning what the key actually is. Here, traditional legal obligations for access to a device would apply and must be respected.

However, "incidental copies" can also refer to situations where incidental copies of the key are generated as a result of a software flaw that allows a hacker (criminal or government) to gain access to the content. Such situations would fall under the analysis on "exploit a flaw", above.

Proposed Workaround: Guess the key

As above, the approach described in the paper raises no additional legal issues that would not arise if a device was not encrypted. Obviously, all human rights safeguards need to be put in place and respected. Further safeguards should also be put in place with regard to the right to access only particular information on a decrypted device, not least due to the extensive and, by default, highly sensitive data that can be stored on or accessed by a device.

Brute force attack

If a police agency lawfully acquires access to ciphertext and can simply try one key after another until one of them works, this would not involve any further invasion of the rights of any person. Should a criminal who uses a weak cipher to conceal her/his plans be taken seriously when s/he objects to the police deciphering her/his plans and using them in evidence against her/him? Curiously, IP owners who protect copyrighted material using weak ciphers expect the law to punish those who exploit their poor engineering, an approach supported in EU and international law (see Article 6.3 of Directive 2001/29/EC, for example). However, when brute force attacks are only possible with the intervention of the provider to undermine the security of the device or service, such activity is tantamount to undermining encryption outright and not a workaround at all.

Proposed Workaround: Compel the key

In this scenario, the user of the device or someone else that has access to the key is legally compelled to give law enforcement authorities access. The Kerr / Schneier paper describes providing a password as "a close cousin of finding the key." While compelling the key may be an acceptable response in some cases, it may also disproportionately interfere with human rights when used improperly.

It is important to note that in any system that allows law enforcement to compel the production of a key, there must be allowances in cases where the individual who used the encrypted device may no longer know the password. A survey conducted by Centrify in 2014 found that a third of people had been locked out of an account due to forgetting a password. In no situation should a person be detained for failing to provide information that they are unable to provide.

In cases where keys are held by third parties, other issues arise. For example, a single key may be used to protect the communications of many individuals, making its production inherently disproportionate. In addition, in any instance where a third party is requested or required to retrieve an encryption key, such surveillance must still comply with user notification principles. Finally, conflict of laws principles must be taken into account where the key that is sought resides in a country other than the one issuing the order.

Social engineering

Social engineering is the action of tricking or manipulating a person to provide information that they would not normally provide. To illustrate this, consider that a criminal could use social engineering to convince a telephone company to reveal personal account information for another person by pretending to be that person and feigning some sort of emergency scenario. Central to social engineering is the concept of deception. This is a long-standing law enforcement practice, but the laws of Member States typically restrict some forms of it. For example, a number of EU Member States consider behaviour that tricks people into betraying their spouses to be in violation of the sanctity of marriage, or the right to respect for her/his private and family life.

Approach 2: Access plaintext, bypass key

In addition to obtaining the key that would be needed to decrypt encrypted information, strategies can also be aimed at bypassing the encryption altogether to gain direct access to plaintext content or data. The following three practices significantly interfere with human rights. These activities essentially use either surveillance or hacking in order to gain access to the plaintext. As described below, there is a dire need for EU surveillance reform, as well as for human rights safeguards to be implemented if and when governments use hacking as an investigation tool.

Proposed Workaround: Exploit a flaw

In the Kerr / Schneier paper, this option is described as "access is gained without requiring the key by exploiting a weakness in the system designed to keep people out." Simply put, this method describes government hacking, and it could often be the most feasible of the six presented workarounds in some circumstances. However, if any government hacking activity is conducted, it must be anchored in a legal framework based around human rights.

Additionally, government stockpiling of vulnerabilities or participating in the zero-day market in an *ad-hoc* basis increases the security and privacy risks faced by individuals and threatens several of their guaranteed human rights. Government agencies should not stock vulnerabilities without an anchored process with rights respecting safeguards and, instead, should disclose vulnerabilities either discovered or purchased unless circumstances weigh heavily against disclosure. Further, they should release reports at least annually on the acquisition and disclosure of vulnerabilities; coordinated vulnerability disclosure should be high on the agenda.

We stress that we have found no examples of governments respecting these principles fully in practice. Therefore, while recognising human rights-compliant government

hacking as theoretically possible, all variations that we have seen in practice fall short of what citizens might reasonably expect.

Government hacking

EDRi member Access Now conducted an investigation into the human-rights implications of government hacking. Following their research and that of other EDRi members, we call for a ban on government hacking practices in principle.

Governments conducting these activities should be mindful of best practices and set up a clear, coordinated vulnerability disclosure system and commit to not stockpiling flaws for future use. The potential adverse effects of this type of stockpiling are exemplified by the Wannacry attack, where unpatched vulnerabilities previously withheld by the US government were used to compromise computers and install ransomware.

Following EDRi-member Access Now's lead, we call for a presumptive ban on the practice until the following safeguards are met:

1. Government hacking must be provided for by law which is both clearly written and publicly available and which specifies the narrow circumstances in which it could be authorised. Government hacking must never occur with either a discriminatory purpose or effect;

2. Government actors must be able to clearly explain why hacking is the least invasive means for getting protected information in any case where it is to be authorised. In each of these cases they must also connect that necessity back to one of the statutory purposes provided. The necessity should be demonstrated for every type of protected information that is sought, which must be identified, and every user (and device) that is targeted. Mass hacking must be prohibited, including not just the hacking of large numbers of devices but also the use of hacking techniques to collect information on large numbers of people from centralised systems.

To illustrate the importance of this safeguard, it is worth remembering that Snowden revealed that GCHQ was harvesting gmail and other Google data in bulk from the backup data flows between Google data centres in different countries. This is no more acceptable

than the EU Data Retention Directive's warrantless and suspicionless collection of the communications data of hundreds of millions of Europeans, which the CJEU found to infringe fundamental rights;

3. Government hacking operations must never occur in perpetuity. Authorisations for government hacking must include a plan and specific dates to develop and conclude the operation. Government hacking operations must be narrowly designed to return only specific types of authorised information from specific targets and to not affect non-target users or broad categories of users. Protected information returned outside of that for which hacking was necessary should be purged immediately;

4. Applications for government hacking must be sufficiently detailed and approved by a competent judicial authority that is legally and practically independent from the entity requesting the authorisation. This judicial authority should also have access to sufficient technical expertise to understand the full nature of the application and any likely collateral damage that may result. Government hacking should never occur prior to judicial authorisation;

5. Government hacking must always provide actual notice to the target of the operation and, when practicable, also to all owners of devices or networks directly impacted by the tool or technique once the investigation phase is finished or otherwise once the national legislation allows the disclosure of this information in analogous situations, such as wiretapping;

6. Agencies conducting government hacking should publish at least annual reports that indicate the extent of government hacking operations, including at a minimum the users impacted, the devices impacted, the length of the operations, and any unexpected consequences of the operation;

7. Government hacking operations must never compel private entities to engage in activity that impacts their own products and services in a way that undermines digital security;

8. If a government hacking operation exceeds the scope of its authorisation, the agency in charge of the authorisation should report back to the judicial authority the extent of and reason for this;

9. Extraterritorial government hacking should not occur absent authorisation under principles of dual criminality and without respecting other principles of international law;

10. Agencies conducting government hacking should not stock vulnerabilities and, instead, should disclose vulnerabilities either discovered or purchased unless circumstances weigh heavily against disclosure. Governments should release reports at least annually on the acquisition and disclosure of vulnerabilities.

Proposed Workaround: Access plaintext when in use

There are two separate components of this activity, including using software such as a keylogger to compromise the physical security of the user's device or either installing physical equipment, such as cameras, into the vicinity of the user to spy on their activity or obtaining a device when it is unlocked, such as when a person is in possession of it. The first scenario is just a different type of government hacking. Whether or not the software or spyware is installed manually or remotely, this sort of interference can have unintended consequences for the user, their device or an entire network. The second scenarios are akin to traditional surveillance and, while they raise few novel challenges, like other workarounds proposed, their use exemplifies deficiencies in rights protections under current laws.

Government hacking

Please see description and safeguards above.

Physical surveillance

Subject to the same safeguards as above.

Proposed Workaround: Locate a plaintext copy

As described in the paper, this option may be possible if such a plaintext copy of the sought-after document exists, including on another device or with another user. This

option does not raise any additional digital rights issues, beyond those already present in accessing any kind of stored electronic data or physical surveillance.

Conclusion

This paper has looked at the issues surrounding the six workarounds proposed in the Kerr / Schneier paper. It is clear that there are multiple challenges that need to be addressed in order to develop thorough evidence-based policy in full respect of national and international human rights safeguards. On the other hand, it has been repeatedly demonstrated that law enforcement agencies are well aware of the discussed practices and many of them are actively in use, enjoying loopholes or absence of national legislation on the issue. These practices directly infringe upon individuals' rights under international legal instruments, including the Charter of Fundamental Rights, and the Commission, in their role as Guardian of the Treaties, has an obligation to investigate and address the malfunctioning *status quo*.

Adopting an acceptable approach requires strong leadership that resists succumbing to the kind of placebo simplistic solutions that have undermined citizens' rights and security as well as evidence-based policy making in this highly politicised policy area. We are committed to helping the Commission to our best ability and capacity in achieving a rights respecting framework for law enforcement access to eevidence.