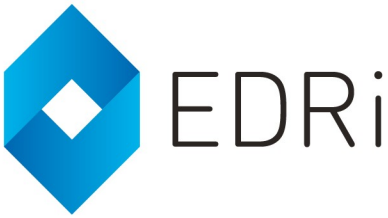

PROTECTING DIGITAL FREEDOM

Position paper on encryption

High-grade encryption is essential for our economy and our democratic freedoms.

Prepared by EDRi member: Bits of Freedom

25/01/2016

High-grade encryption is essential for our economy and our democratic freedoms

A summary of some basic concepts surrounding encryption can be found in the EDRi booklet "How the Internet works.[1]

The availability and use of high-grade encryption is essential for the protection of our digital infrastructure and communications. It is not only important for our democratic freedoms, but also vital for innovation and economic growth.

Therefore, all governments must:

- stimulate the development of high-grade standards for encryption,
- stimulate the use of high-grade encryption, and
- not in any way undermine the development, production or use of high-grade encryption.

By extension, no government should set limits on the maximum length of encryption keys,[2] compel the installation of vulnerabilities for use by the government (such as backdoors),[3] require the creation and/or handover of master encryptions keys,[4] restrict the export or import of encryption technologies, or take any other step that blocks development and use of high-grade encryption.

Our economy needs high-grade encryption

The stimulation and use of high-grade encryption promotes trust in our digital infrastructure and communications. It protects our sensitive personal data, company secrets, and government interests, and makes economic espionage more difficult.

Explicitly choosing to promote high-grade encryption standards strengthens the international competitive position of any country. Given the option, users – whether consumers or businesses – will always choose to place their sensitive information with companies that use high-grade encryption. If one country undermines the use of high-grade encryption, companies that depend on strong security for their sensitive information and communications will relocate to another country. A country that stimulates the use of high-grade encryption strengthens its investment climate.[5]

Mandating the use of weak encryption will create huge burdens for businesses. Companies will need to make additional investments in order to comply with the requirement to use only weak technology in specific markets. International companies will still have to invest in strong encryption in order to protect their customers in other countries and to satisfy the requirements of other jurisdictions. This additional investment slows down innovation because products will need to satisfy more requirements.

In addition, it sets a dangerous precedent: if one country forces companies to use weak encryption, other countries will follow suit. If, for example, the Netherlands wants access to the vulnerabilities in the software developed by, say, the Chinese, China will want access to the vulnerabilities in the software developed by the Dutch. The burden on international companies will increase, products will become more vulnerable, and the risk of economic espionage will rise.

Added to this is the risk of liability in case of misuse. The installation of backdoors means that companies must trust the producers of the vulnerabilities. This creates uncertainty regarding who is liable if criminals take advantage of the vulnerabilities to steal from end users or get their hands on company secrets.

Governments also benefit from high-grade encryption

Citizens submit digital tax returns; the intelligence community encrypts state secrets; the army sends orders securely in order to avoid compromising military operations and civil servants negotiate trade deals by sending messages that only the addressee can read. All of this would be hard to realise without encryption ensuring authenticity, integrity and confidentiality of information.

Our freedoms are enhanced by high-grade encryption

The ordinary citizen depends upon high-grade encryption standards. The protection of digital communication is essential for a citizen's autonomy in any modern democracy. Encryption enables citizens to collect information and communicate with others without outside interference. Encryption is an increasingly fundamental building block for freedom of expression and respect for privacy as enshrined in international treaties such as the European Convention on Human Rights.

Technical: encryption cannot be weakened "just a little"

If the choice for high-grade encryption standards is not made unconditionally, a path is forged that is counter to the general perception that the security of our digital ecosystem needs to be strengthened. A policy mandating weak standards would impede the further development of high-

grade encryption, such as keys that are generated with each session.[6] This would be no different if companies are required not to use end to end encryption any more.

Encryption cannot be weakened without potentially introducing additional vulnerabilities.[7] The installation of intentional vulnerabilities increases the complexity of the software. This is significant because complexity and security are inversely related to each other: anyone who intentionally creates vulnerabilities, also creates unintentional vulnerabilities.[8] It's not just about technical vulnerabilities. When a backdoor is broadly implemented, hundreds of developers will know about the architecture. The additional functionality serves to increase the number of ways that security can be breached, broadening the so-called "attack surface".

A built-in vulnerability can be used by anyone. It is technically impossible to build a vulnerability that can be used only by police investigators and intelligence services from a specific country.[9] Sooner or later, a secret vulnerability will be cracked by malicious users.[10] This is no different when using "golden keys". Such keys give access to a massive amount of highly sensitive information. The keys themselves become an especially attractive target for attack.

Once built, such weaknesses in software can haunt us for decades. A number of serious vulnerabilities discovered in security software in recent years were ordered by governments decades ago.[11]

A ban on high-grade encryption cannot be enforced. The number of possibilities for criminals to evade government-ordered restrictions on encryption are infinite.[12] Knowledge of high-grade encryption already exists, and its further development and use cannot be prevented. As a result, only innocent individuals, companies, and governments with weak encryption standards will suffer.

Or, as the cryptographer, Philip R. Zimmermann said,

> "When crypto is outlawed, only outlaws will have crypto."[13]

1 Available from https://edri.org/wp-content/uploads/2013/10/paper03_web_20120123.pdf

2 Between World War II and the 1990's, the American government limited the export of encryption keys longer than 40 bits. Other countries had to accept weaker forms of encryption: just about good enough for low value shopping transactions on the Internet, but weak enough that the security service could undo the encryption. This limitation was finally lifted due to fears about the consequences on economic growth.

3 Sometimes called front doors.

4 Known as "key escrow", "key recovery" and "trusted third-party encryption".

5 A number of companies have expressed highly negative views about the investment climate in the Netherlands in response to the recently proposed Security Act. Telecom company Voys said "If you value your customers' privacy, don't start up in the Netherlands [...]"

6 A concrete example is "forward secrecy", a technique in which keys are destroyed after use. Thus, keys that are stolen cannot be used to intercept communications sent either earlier or later. If manufacturers are required to include an extra key so that the government can unlock communications, the disadvantages of "forward secrecy" are lost.

7 See also "Keys under Doormats" report by fifteen renowned cryptographers, amongst them Ross Anderson, Matt Blaze, Whitfield Diffie, Matthew Green, Ronald L. Rivest and Bruce Schneier.

8 In the 1990s, the American government introduced a backdoor, "the Clipper Chip", which had to be installed in all kinds of systems. Cryptographer Matt Blaze showed that this deliberate vulnerability itself contained a vulnerability.

9 Equipment from the American company Cisco contained vulnerabilities installed to allow investigation and intelligence services access to internet traffic handled by these devices. This functionality contained leaks that were exploited by attackers.

10 In Greece, legal call-intercept functionality that was intended for use by law enforcement was hacked. The perpetrators illegally eavesdropped on the conversations of more than a hundred members of parliament and high-ranking civil servants. This illegal wiretapping began in the summer of 2004 and was not discovered until the following spring. A more recent example is Google's interface, which gives law enforcement and secret services access to Google's customers' data. This database of which customers were being monitored was accessed by the Chinese secret service to determine if their spies were known to the American government.

11 The restrictions on the export of encryption technology in the 1990's are still causing problems today. Even though the restrictions were lifted almost two decades ago, the weak encryption code was, for understandable reasons, never removed – it was forgotten. In 2015 it became clear that malicious hackers could exploit the forgotten code. Investigators discovered two vulnerabilities, known as FREAK and LogJam, whereby systems could be fooled into using the weak encryption, which, with the speed of modern computers, is almost trivially easy for attackers to decrypt..

12 See "You can't backdoor a platform" by Jonathan Mayer. For example, if the government required Google to install a backdoor in the operating system of Android telephones, Google would need to weaken the encryption on the hard drive in the telephone. But that leaves third party applications untouched. Google would have to address every application on its platform. Even that would not prevent the user from installing another application via another app-store. It is a battle that cannot be won.

13 See "Crypto: How the code rebels beat the government – saving privacy in the digital age" by Steven Levy, 2001, page 198.