RIGHT TO ENCRYPTION INSTEAD OF A MASTER KEY FOR ENCRYPTED COMMUNICATION

1. BACKGROUND

The governments of the EU countries are preparing a resolution in the Council of Ministers currently titled "Draft Council Resolution on Encryption-Security through encryption and security despite encryption"[1]. It shows clear resemblance to earlier initiatives to force providers of end-to-end encrypted communication to keep a "master key" for enabling "competent authorities" access to electronic evidence [2], [3].

The draft declares "The European Union fully supports the development, implementation and use of strong encryption. Encryption is a necessary means of protecting fundamental rights and the digital security of governments, industry and society. At the same time, the European Union needs to ensure the ability of competent authorities in the area of security and criminal justice, e.g. law enforcement and judicial authorities, to exercise their lawful powers, both online and offline." "Protecting the privacy and security of communications through encryption and at the same time upholding the possibility for competent authorities in the area of security and criminal justice to lawfully access relevant data for legitimate, clearly defined purposes in fighting serious and/or organized crimes and terrorism, including in the digital world, are extremely important. Any actions taken have to balance these interests carefully."[1]

However, while the fundamental right to encryption is essential for Europe's democracy - just as postal and telephone secrecy was in the analogue world, secret communication can neither be effectively prevented with a master key nor with an encryption ban. Criminals could switch to unobservable communication with steganography[1]. Moreover providing backdoors into communication, on the one hand, opens the possibility of ongoing access for government agencies and on the other hand, does not reduce the ability for criminals to encrypt their communication.

The planned weakening of end-to-end encryption and protection of communication is claimed to be justified due to current terrorist attacks in France and Austria, although, according to current knowledge, encrypted communication played no role in either in the preparation or in the investigation of these crimes.

Already in the 1990s, the US government wanted to ban the export of encryption programs and demanded manufacturers to implement backdoors. However, this did not hinder the spread of encryption, e.g. the software "Pretty Good Privacy"(PGP) [4].

2. CONCERNS

The initiative endangers not only the informational self-determination of EU citizens but also the protection of company and business secrets. Undermining the efforts towards legally binding corporate communication by weakening encryption, is ultimately hindering the necessary digitalization of the European economy, on top of that need reliable, confidential communication for the formation of political will and the creation of a free society.

Encryption helps to adequately protect the values on our ICT systems and thus to go into a safe and trustworthy digital future. To weaken encryption means to endanger the digitization in the EU. Therefore, it is important to promote trust in ICT, not to reduce it.

The “balance” to make encryption secure and officially interceptable at the same time is an illusion. And from a cryptographic point of view, there are no "good" or "bad" attackers. Thus, competent

[1] Hiding secret messages in other unsuspiciously looking messages https://en.wikipedia.org/wiki/Steganography

cybersecurity authorities agree that weakening encryption technology and purposely built backdoors are entirely contrary to the principles of cryptography – secure encryption means that only those who control data can access it [6], [7]. In many cases cybercrime authorities have already now tools like online Trojans at hand that can give them insight into encrypted communication at the respective endpoint.

The draft European Council proposal does not state how the access tools and the accessed data would be protected. However, the protection of such instruments and the related data is an issue of great sensitivity, as many parties may be interested in it. In the digital sphere, weaknesses, leaks, and leaked data scale differently from how they do in the analogue sphere. Once somebody has accessed leaks and leaked data, they very quickly reach others. For information and data, one can see this with, e.g., posts going viral in social networks. For technology weaknesses and keys, one could see it in the field of digital content protection, where keys and information about weaknesses of protection mechanisms spread rapidly. Thus, this can broaden the possibilities for uncontrolled access by countless consumers and secret services from home and abroad to communication between EU citizens. Weakening or even removing adequate encryption is problematic and endangers large numbers of users, including journalists and human right activists.

Solutions with back doors cannot be considered as 'state of the art and "master keys" endanger the liberal, constitutional state. If large numbers of duplicate keys fall into the wrong hands, this could lead to disaster. Removing strong end-to-end encryption creates vulnerabilities that can be exploited not just by EU government agencies, but also by anybody – including hackers, cybercriminals and state-sanctioned operatives from foreign governments – with the technical ability to discover that purposefully created backdoor.

3. RECOMMENDATIONS

The Council of European Professional Informatics Societies (CEPIS) calls on the German Federal Government as the current Council Chair, the European Commission, and the European Parliament to vehemently oppose this proposal to weaken end-to-end encryption and instead advocate a European "right to encryption".

A “master key”, as demanded by the Council of Ministers draft, undermines trust in such encryption and endangers the growth of the European ICT industry and the goal of European technological sovereignty. CEPIS, therefore, calls on the Commission and Parliament to counter the proposal of the Council of Ministers with a strong European right to encryption.

The European Commission and Parliament are also called upon to stand up for European data protection. With the General Data Protection Regulation (GDPR), the Union has managed in recent years to create a competitive advantage for the European digital economy and laid the foundations for its technological sovereignty. For example, GDPR Art. 32 explicitly obliges to "encrypt personal data".

Additionally, it is possible to fight terrorism and other forms of serious crime consistently, but backdoors in communication services cannot be the solution for this. Anyone who weakens encryption weakens ICT security as a whole. Namely, criminals can switch to services that cannot be reached with EU laws. A solution could also be to include more qualified employees in authorities who can investigate in the digital space.

References

[1] Council document 12143/1/20 REV1 "Draft Council Resolution on Encryption-Security through encryption and security despite encryption" https://www.heise.de/downloads/18/2/9/9/8/5/2/0/783284_fh_st12143-re01en20_783284.pdf, earlier version on https://www.heise.de/downloads/18/2/9/9/8/5/2/0/eu-council-draft-declaration-against-

encryption-12143-20.pdf, some background on https://blog.lukaszolejnik.com/the-policy-of-security-despite-encryption/

[2] How a Crypto 'Backdoor' Pitted the Tech World Against the NSA, WIRED, https://www.wired.com/2013/09/nsa-backdoor/

[3] Backdoors – A Few Thoughts on Cryptographic Engineering, Matthew Green, https://blog.cryptographyengineering.com/category/backdoors/

[4] Why I Wrote PGP?, Philip Zimmermann, https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html

[5] Keys under doormats: mandating insecurity by requiring government access to all data and communications, Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael A. Specter and Daniel J. Weitzner; Journal of Cybersecurity, 1(1), 2015, 69–79, DOI: 10.1093/cybsec/tyv009; https://academic.oup.com/cybersecurity/article/1/1/69/2367066

[6] The Importance of Strong Encryption to Security, Bruce Schneier, Schneier on Security, https://www.schneier.com/blog/archives/2016/02/the_importance_.html

[7] ENISA's Opinion Paper on Encryption: Strong Encryption Safeguards our Digital Identity, European Union Agency for Network and Information Security (ENISA), https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-opinion-paper-on-encryption