Position Paper

Protect end-to-end encryption

10. November 2020

Secomba GmbH

Werner-von-Siemens-Str. 6
86159 Augsburg
Deutschland

T 0049 (0) 821 90786150
www.boxcryptor.com
info@boxcryptor.com

Registered Office
Augsburg, HRB 26138
Amtsgericht Augsburg

Management
Andrea Pfundmeier
Robert Freudenreich

Summary

Confidential Communication is fundamental for our liberal democratic society and must therefore be preserved at all cost.

End-to-end encryption always comes under fire when complex problems need to be tackled with simple means. Terror and child abuse are terrible crimes but must be fought at its roots. It is disproportionate to abandon IT security of all citizens for this reason.

Demands

- Demand 1: Fight crime at its root cause and take preventive measures instead of relying on data retention and algorithms as a panacea.
- Demand 2: Prevent the blur between law enforcement and civil society.
- Demand 3: Provide law enforcement agencies with better financial and human resources and enhance networking between authorities.

What is end-to-end encryption?

Many internet service providers encrypt the uploaded content of their users. This is part of their service, whether it concerns cloud storage, chat services, or banking apps. However, as long as the entity that implements the encryption is also in possession of the key, providers can still access the content at any time. In the US they can even be forced by authorities to get access to unencrypted files. This is regulated in the so-called CLOUD Act.

With end-to-end encryption, each user encrypts their content and shares the key only with other authorized people. This way, you can ensure that only these authorized people have access to data in plain text.

End-to-end encryption is necessary, for example, to communicate securely, to protect business secrets or to meet the requirements of the GDPR for the protection of personal data.

What is a threat to end-to-end encryption? Current discussion points.

In the US, with the EARN IT Act and LAED Act, two laws are aiming to prohibit end-to-end encryption. Given that most major internet providers are based in the US, this ban will also affect many EU citizens.

Currently, however, there are also voices within the European Union calling for a similar law to the EARN IT act. These include Counter-terrorism Coordinator Gilles de Kerchove and European Commissioner for Home Affairs Ylva Johansson.

Is there a technical solution?

By searching for officially known hashes (mathematical imprints) of illegal images and video material during the upload of a file, providers are able to recognize and report those files before they are published. This procedure only works if the hashes of files are never modified.

However, end-to-end encryption implements modifications which would make automatic scanning useless. This problem can only be solved by “undermining” the strong encryption.

Nevertheless, no procedure allows a “weakened” form of end-to-end encryption — diluting is equivalent to abolishing it. This is also made clear in the paper with which the EU Commission opened the discussion on end-to-end encryption: You can only maintain or abolish end-to-end encryption.

Demands

Freedom of expression and the right to privacy for the entire population must not be infringed to prosecute individual offenders.

Please take three of our demands into consideration:

Demand 1: Fight crime at its root and take preventive measures instead of relying on data retention and algorithms as a panacea.

Two motives are repeatedly cited as the reasons for abolishing end-to-end encryption: protection against terrorism and the prosecution of people who share and collect images of child abuse on the internet. For both problems, effective preventive measures from various specialists are available. We advocate to fight the causes and to better equip specialized organizations instead of relying on surveillance and data retention.

Demand 2: Prevent the blur between law enforcement and civil society.

Currently, companies in Germany are forced to delete allegedly illegal comments within the regulations of the NetzDG. The decision whether a comment is illegal is therefore made by algorithms and employees of the respective companies instead of law enforcement agencies. This may be appropriate for crimes like sedition. But in complicated cases such as insult, even courts often decide divergent. As a result, platforms tend to delete too much rather than too little since there are no penalties for accidentally deleted content.

After only a short time, the governments of Belarus, India, Malaysia, and Russia copied the NetzDG. Prof. Dr. Wolfgang Schulz calls the law a negative export hit.

The establishment of a similar approach for encrypted contents must be unconditionally prevented. Companies operating with commercial interests should not be the extension of governments or prosecuting authorities.

Demand 3: Provide law enforcement agencies better financial and human resources and enhance networking between authorities.

Amplified by data retention, but already prior to it, complaints emerged from police and law enforcement about the sheer flood of unmanageable work. Unappealing jobs are also causing a shortage of skilled workers in the IT departments of police authorities. With progressing digitalization “Internet crimes” are also rather increasing. We call for a retrofit and an increase of personnel.

Lack of networking between law enforcement agencies in different countries and federal states has led to several investigation breakdowns in the past. Improvements are needed, and an adaption of federalism to the digital age is urgently recommended.

Conclusion

Investigations into terrorism and child abuse are always cited as a reason to get rid of end-to-end encryption. We believe that crimes of individuals must be fought against, not the privacy of all.