# Developing security protocols for misuse-resistant digital surveillance

November 14 2023

Credit: Pixabay/CC0 Public Domain

Privacy is gaining importance in our digital society. There is a strong demand for anonymity and confidentiality of data according to the European General Data Protection Regulation.

On the other hand, laws and directives, such as the Resolution of the European Council on the Lawful Interception of Telecommunications or the EU Directive on the Fight against Money Laundering and Terrorist Financing, require the revocation of anonymity or uncovering the users' encrypted communication under certain, precisely defined circumstances, e.g., when surveillance of suspects is ordered by a judge. Consequently, many applications are subject to requirements or regulations restricting unconditional anonymity.

## Illegal mass surveillance via the backdoor

The problem of such "digital backdoors," however, is that they allow for unnoticed mass surveillance. Hence, independent, trustworthy offices are required for the surveillance of surveillants. Moreover, a system is needed to force a court order that cannot be changed later on when the backdoor is to be used in order to ensure the lawfulness of this measure. Existing systems are lacking strict technical mechanisms.

"We have developed security protocols that can do both: They enable surveillance of encrypted or anonymous communication and, at the same time, prevent or at least uncover illegal surveillance," says Dr. Andy Rupp, Head of the Cryptographic Protocols Group of the KASTEL Security Research Labs of KIT. "We want to significantly increase the trust of the public in the honesty of operators and prosecution authorities."

## Controlled use of digital backdoors

The research team developed a module for auditable surveillance. This security protocol protects users in several ways: Digital backdoors open for a short time and for specific users only. They are shared by trustworthy parties, and access to them is provided under certain

conditions only.

Moreover, users are technically forced to leave unchangeable documents when opening the backdoors. This allows for a later check of the lawfulness of surveillance by an independent auditor and for publicly verifiable statistics on the use of backdoors.

Potential applications of these auditable surveillance systems range from mobile communication systems, such as 5G and instant messaging services, to electronic payments to legal video surveillance. "We have developed a first auditable surveillance concept. Several technical and legal challenges remain to be studied before it will be used in practice. This will be the subject of our future interdisciplinary research," Rupp says.

**More information:** Universally Composable Auditable Surveillance. Accepted for the 30th International Conference on the Theory and Application of Cryptology and Information Security—ASIACRYPT, 2023 eprint.iacr.org/2023/1343

Provided by Karlsruhe Institute of Technology