Client-side scanning is like bugs in our pockets

October 19 2021, by Sheena Kennedy

An artificially constructed pair of images built to intentionally create a false positive, where the dog is detected as the girl. Credit: Ecole Polytechnique Federale de Lausanne

Encryption provides a solution to security risks, but its flipside is that it can hinder law enforcement investigations. A new technology called client-side scanning (CSS) would enable targeted information to be revealed through on-device analysis, without weakening encryption or providing decryption keys. However, an international group of experts,

including EPFL, has now released a report raising the alert, arguing that CSS neither ensures crime prevention nor prevents unwarranted surveillance.

With end-to-end encryption, your data is protected at each end and in transit. While CSS doesn't interfere with this encryption, it scans your content ahead of transmission, right on your device. The way it is pitched, law enforcement would limit these searches to "targeted material," that is, material that is clearly illegal. When there is such targeted material on a device, its existence and potentially its source would be detected, thereby enabling crime prevention while allowing legal private communications to pass unimpeded.

Proponents say CSS should be installed on all devices, not just when there is good reason to suspect criminal use of communications, arguing that this is needed for effective policing and does not infringe on user rights. "There is a false sense of security because end-to-end encryption is still used," explains EPFL's Carmela Troncoso, one of the report's authors. "In fact, with universal deployment, the end-to-end encryption means nothing because the content in your device has already been scanned."

While supporters say CSS can give users control since it happens on their own devices, this makes it less, not more secure. "Our everyday devices have weak spots that can be abused," explains Troncoso, a tenure track assistant professor of security and privacy. "It would be difficult to ensure that only authorities would be doing the scanning, and only in agreed-upon ways. It would be difficult to ensure that only so-called targeted material is being scanned. Plus, unlike other monitoring methods, once CSS is in place it isn't necessarily limited to communications. It can be expanded to any material in the phone whether you intend to share it or not."

If CSS is implemented universally, and without due consideration for the vulnerabilities of user devices, the result would be an "extremely dangerous societal experiment." There are many who would be quick to jump through this open door, as has been shown, for example, with cyber interference in elections.

Cracks in the CSS idea include potential abuse by authorized parties, abuse by unauthorized parties and attacks by people close to the user, such as a controlling ex-partner or a school bully. Privacy risks start with the ability of the system to go beyond communications, revealing content in other device components on purpose or by accident. And the slope with CSS only gets slipperier. The definition of "targeted content" is in question. Child sex-abuse material is an evident first item on the list, clearly considered a crime. You may add terrorism and organized crime to the list, as the EU has. Divergent definitions and gray areas quickly follow.

Alongside the privacy and security drawbacks raised by the authors is the observation that CSS is not efficient and effective as a crime-fighting tool. Because matching algorithms are not exact, the false matches can create problems. There are also several paths to deliberate evasion: Those who want to can disguise targeted material in ways that thwart effective machine learning-based matching, or clog up the system with false positives such that detections are meaningless.

Some service providers are working on ways to provide CSS capabilities while enabling some privacy for users. Yet so far, the authors conclude, the protection of their propositions is illusory.

The report's authors also identify many practical blocks to deployment—concerns for fairness and discrimination, technical and bureaucratic blocks, policy questions, jurisdictional issues and a fundamental incompatibility between secrecy and accountability.

Delving into the architecture of CSS, the authors conclude that it would not be possible to deploy CSS safely.

"The checks and balances that limit the scope of previous surveillance methods in democracies just aren't there with broad deployment of CSS. As law-abiding citizens, we should be free to use our devices to make our lives easier, without worry of being bugged like a spy movie villain," says Troncoso. "It's freedom of speech, it's at the heart of what we consider democracy. Yes, curbing crime is critically important. CSS just isn't the way to do it."

More information: Hal Abelson et al, Bugs in our Pockets: The Risks of Client-Side Scanning. arXiv:2110.07450v1 [cs.CR], arxiv.org/abs/2110.07450

Provided by Ecole Polytechnique Federale de Lausanne