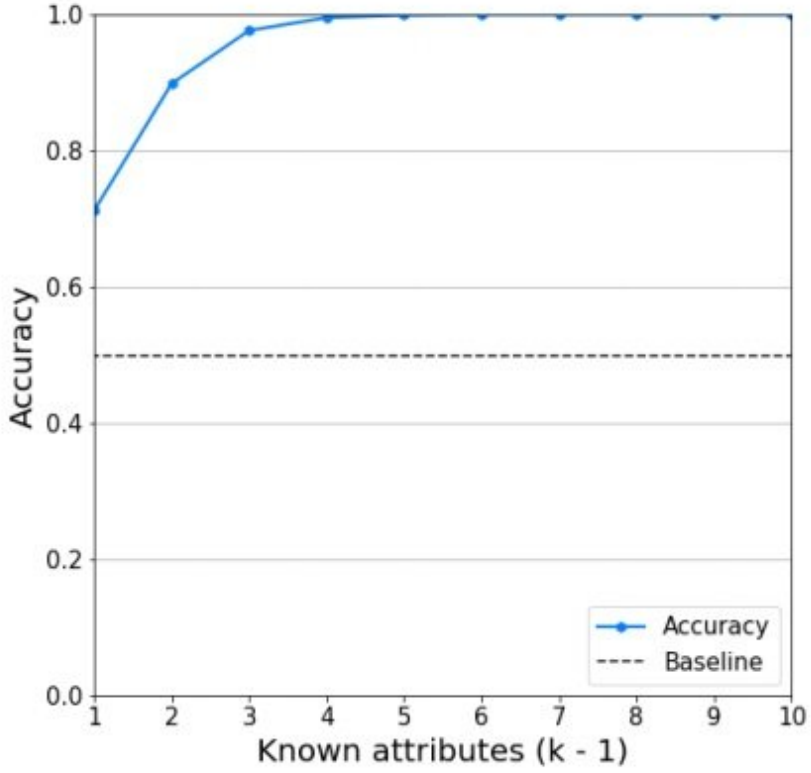
Researchers' attack on data privacy system shows noise leaks the very data it is trying to protect

May 1 2018, by Lisa Zyga



In the noise-exploitation attack, researchers can determine an individual's private information with high accuracy by knowing only a few attributes about the individual. Credit: Gadotti et al.

Demonstrating just how challenging it is to keep private data secure, researchers from Imperial College London have presented an attack on a new data privacy system called Diffix, whose breakthrough technology has recently been commercialized and approved by the French data protection authority CNIL to satisfy the full criteria for GDPR (General Data Protection Regulation)—the new EU data protection law set to go into effect at the end of May.

But now the researchers have shown that, using only five attributes of an individual and asking 10 carefully chosen questions to the query-based system, it's possible to determine the individual's private attributes with up to 99% accuracy.

The researchers, Andrea Gadotti, Florimond Houssiau, Luc Rocher, and Yves-Alexandre de Montjoye from the departments of computing and data science at Imperial College London, have written a paper on their noise-exploitation attack on Diffix, which was developed by the German start-up Aircloak. Diffix uses technology pioneered by researchers at the Max Planck Institute over several years.

As the researchers at Imperial College London explain, the purpose of their attack is to highlight the need for both the full transparency of all new data privacy systems, along with a community that has full access to the techniques in order to detect and discuss potential vulnerabilities.

"We need to accept that no system is perfect," the researchers write in their blog at the Computational Privacy Group. "There will be attacks, and some of them will succeed. We need to prepare for this and learn from best practices in security: ensuring that several layers of security exist, to not have all the data in one place (what Jean-Pierre Hubaux calls the Fort Knox approach), etc. We also need standards and systems to be completely transparent and open. Building secure systems requires anyone to be able to review the code without technical or legal barriers,

propose solutions and build upon existing work."

Data privacy protection systems are rapidly evolving, with traditional approaches based on data anonymization now rendered obsolete, due in part to the large sizes and uses of modern datasets. Alternatives to data anonymization, such as query-based systems like the one used by Diffix, provide a promising new solution. In these systems, users can ask questions about the data system and receive aggregate results as answers. This method aims to find a balance between using the data for useful purposes, such as performing research and fighting disease, while maintaining individual privacy.

In Diffix, the privacy protection comes in large part from the addition of noise. Somewhat ironically, the researchers exploit this noise in their attack in order to infer private information of individuals in the database. To do this, they implement an intersection attack, in which they pose two queries that ask for the number of individuals in the dataset who meet certain conditions. The two queries differ by only one condition, so that by calculating the difference between the results it's possible to cancel out part of the noise. The researchers showed that, by obtaining five pairs of these results, and then performing a statistical test (the likelihood ratio test), it's possible to determine certain information about an individual—for example, whether or not the person has HIV.

Although the researchers point out a few limitations of their attack, they believe that it exposes a serious vulnerability of the system, and provides a reminder that privacy protection will continue to be an ongoing challenge.

More information: Andrea Gadotti, Florimond Houssiau, Luc Rocher, and Yves-Alexandre de Montjoye. "When the signal is in the noise: The limits of Diffix's sticky noise." To be published. arXiv:1804.06752 [cs.CR]

Abstract
Finding a balance between privacy and utility, allowing researchers and businesses to use data for good while protecting people's privacy, is one of the biggest challenge we face today. A large body of research has shown the limits of the traditional anonymization (or de-identification) model prompting the use of question and answer or query-based systems. Diffix is a query-based system developed by Aircloak using the concept of "sticky noise" to protect people's privacy. We here present an attack on Diffix that exploits the structure of its sticky noise to infer private attributes of people in the dataset. We believe this vulnerability to be serious, allowing us to accurately infer private information of users with little background knowledge. While we share Diffix's creators view that we need to take a fresh look at building practical privacy-preserving systems, we believe this requires a layered security approach and fully open tools and discussions. Patented and proprietary code is unlikely to be sufficient to truly help us find a balance between the great potential of data and the basic human right of privacy.

Additional information: Response from Aircloak:

Technical explanation of what has happened by Paul Francis, Director at Max Planck Institute for Software Systems:
https://blog.aircloak.com/report-on-the-diffix-vulnerability-announced-by-imperial-college-london-and-cu-louvain-7c558207b2f3

Statement by Aircloak managing director Felix Bauer:
https://blog.aircloak.com/statement-regarding-the-attack-on-diffix-by-imperial-college-scientists-d927d3b25114