

Researchers explore possibilities for an ultra-secure gun registry

15 March 2021, by Kevin Stacey



A research team led by Seny Kamara, an associate professor of computer science, has proposed an ultra-secure and decentralized gun registry database. Credit: Nick Dentamaro/Brown University

Proposals to create a national gun registry have long been met with fierce opposition from gun rights advocates. While proponents say a registry would help in tracking guns used in crimes, opponents worry that it would compromise privacy and could be used by the federal government to confiscate firearms. Now, a team of Brown University computer scientists has devised a way of implementing a registry that may allay some of those concerns.

They propose a database that uses advanced encryption to protect privacy. The encryption scheme allows the database to be searched without being decrypted, which means people querying the database see only the records they're looking for and nothing else. Meanwhile, the system places control of data in the hands of county-level officials rather than the federal government, meaning county officials have control over which queries are answered, and can even pull the county's data offline entirely if they're not

comfortable with how it's being used.

The proposed system is the work of Seny Kamara, a professor of computer science at Brown, along with co-authors Tarik Moataz, Andrew Park and Lucy Qin. Moataz is a visiting scientist at Brown. Park is a Brown master's student, and Qin is a Ph.D. student in Kamara's lab. They developed the system after Ron Wyden, a U.S. Senator from Oregon, contacted them looking for ideas on how such a database might be constructed.

"The senator's office had this idea for a database where counties are incentivized to participate, but they could pull out at any time," Kamara said. "At the same time, there are obvious privacy concerns. This idea of being able to query and [process data](#) without decrypting it is something I have worked on for the last 20 years, so that's why the senator reached out to us. This research was about showing whether it was possible to design something like this."

The study, which was accepted to the IEEE Symposium on Security and Privacy and will be presented in May, concludes that such a system is not only possible, but quite practical.

The proposed registry would contain the make, model and serial number of all legally owned guns in each participating county, along with a registration number identifying gun owners. The information in each county database would be fully encrypted, and only a designated county official would hold the key to decrypting their own local data.

Each county's encrypted data would be searchable by authorized users elsewhere (authorized users would include [law enforcement](#), county officials or gun sellers). For example, a law enforcement officer might query the system with the serial number of a gun found at a crime scene. Without ever decrypting the data, the system would locate

the county database containing that [serial number](#). The officer would then be able to decrypt the relevant record, as long as the country official controlling the data has enabled it to do so.

The [search algorithm](#) provides a high level of security because the data is never decrypted during the search process.

"All of the servers that are storing the data and all of the computers that are doing these operations, they're just processing encrypted data and they never actually see anything," Kamara said. "That provides really strong privacy throughout the process because none of the data can ever be seen without the decryption key."

Kamara and his colleagues envision the decryption key as a physical device—like a thumb drive—that can be placed in a local computer to authorize transactions.

"If at some point a county decides they don't want to be part of the system anymore, the official just pulls that hardware token out of the laptop and that's it—nothing works," he said. "The data is encrypted and the key is unavailable, so nothing can happen. For the senator's office, that ability for counties to walk away and basically pull their data offline was really important."

For their study, the researchers created a mock-up of the database with synthetic data and showed that searches were computationally practical, with results returned in a minute or less. The analysis also found that the costs associated with the system would be relatively small. Each county [database](#) could be stored for less than \$1,000 per year, and the global directory would cost less than \$500 per year.

Kamara says that the work so far is a proof-of-concept that would require some additional refinement to be implemented. But as it is, he says, the work shows the value of bringing technical expertise to bear on policy issues.

"I think people imagine this registry and think everything would be public and there would be all kinds of problems associated with that," he said.

"But with advanced cryptography, that's not necessarily true. So I think this is an example of how you can have technology folks and policymakers working in concert, and it changes the conversation. It's been a really great collaboration."

More information: Seny Kamara et al. A Decentralized and Encrypted National Gun Registry: eprint.iacr.org/2021/107.pdf

Provided by Brown University

APA citation: Researchers explore possibilities for an ultra-secure gun registry (2021, March 15) retrieved 24 October 2021 from <https://techxplore.com/news/2021-03-explore-possibilities-ultra-secure-gun-registry.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.