Smartphones set out to decipher a cryptographic system

August 25 2014, by Sébastien Corthésy

Ramasany Gowthami. Credit: Alain Herzog / EPFL 2014

While carrying out her master thesis on computer science, Ramasany Gowthami participated in the creation of an Android app by means of which users get together to crack a modern cryptographic code.

Modern cryptography is not infallible. All encryption types, among which we can find the widely used RSA, can theoretically be broken. If so, how to ensure that our data remains protected? The answer lies on the time and computational effort required to break the code. Cracking a sufficiently long encryption key can be expensive up to the point of being unattainable in practice.

The LACAL laboratory at EPFL, renowned for its many achievements

in the field of cryptography and led by Arjen Lenstra, was interested in solving a problem based on elliptic curve cryptography developed in the early 1980s. After having thwarted the security of our passwords by using a network of 300 PlayStation 3 game consoles, the researchers decided to take on this new challenge, on this occasion by using thousands of smartphones working together. "All of us do not necessarily have a computer for running the algorithm, making it difficult to gather a few dozen. On the other hand, everyone has a smartphone, and launching the application becomes a child's game!" said Ramasany Gowthami, a master student in computer science that participated on the project. By running the algorithm a very large number of times the code may be broken eventually. To do this, users simply launch the application and press a button. The app also allows users to register, form teams, view their statistics and thus measure their participation in this unprecedented undertaking.

Despite her apprehension about the mathematical part of the project, Ramasany Gowthami does not regret having plunged into this domain for her master's thesis. She acknowledges that the part of the implementation of which she was in charge required long working weeks to get to understand the whole project. "Since I was in charge of the interface between the program's components, I had to have a perfect knowledge of the elements of the algorithm," she explains. "What is my best memory? When I managed to put it all in my head and was able to grasp the entire project! ".

Why this desire to crack an unbroken cryptographic system at all costs? "It's just as important as designing new and more efficient systems," she explained. "We know that the systems can be broken at some point. That's why it is important to constantly assess them in order to know their limitations and adapt them if they are no longer safe. This can be done, for example, by extending the length of the encryption key. Perhaps a similar evaluation work on the SSL would have prevented the

(in) famous Heartbleed bug!"

Provided by Ecole Polytechnique Federale de Lausanne