Vuvuzela, a next-generation anonymity tool that protects users by adding NOISE

December 18 2015, by Martin Berger

Communicating by Vuvuzela, for when anonymity could be a matter of life and death. Credit: e3000, CC BY-SA

Cryptography is the science of keeping secrets, with encryption algorithms and methods such as public key encryption the gold standard. Despite widespread usage and heavy scrutiny, these ciphers remain unbroken. But while encryption can keep messages secret, it cannot protect the identities of the sender and receiver.

Details such as the IP addresses of computers communicating on the internet and other metadata can reveal more than just the identities of those communicating. Companies use metadata to infer sexual orientation, approximate age, gender and interests for targeted advertising, while intelligence and law enforcement agencies collect and analyse it for their own uses. As a former director of the NSA puts it pithily: "We kill people based on metadata."

So anonymity is required as well as secrecy, for which the most polished tool is Tor. Tor allows users to browse the web anonymously, but has come under sustained attack – and cracks have begun to show. Is it time for a replacement? Vuvuzela, a prototype anonymising software designed by MIT researchers, is one attempt.

Tor achieves anonymity by partially encrypting as much metadata as possible, revealing only small amounts and only as late on in the communication as possible. It sends messages via the encrypted Tor network, where it's difficult for attackers that snoop on network traffic to detect where a message comes from and where it is going. That an NSA presentation leaked by Edward Snowden included the statement "Tor Stinks" suggests that even the NSA found it difficult to crack.

Yet when the FBI shut down the Silk Road and Silk Road 2.0 illegal online marketplaces, their prosecutions seemingly relied on evidence collected despite Tor's privacy measures. Tor has well-known security weaknesses which are explicitly stated by the developers. One is that Tor cannot withstand traffic analysis by an attacker who can monitor global

internet traffic in real time: whenever user A sends a message to Tor and almost immediately afterwards Tor sends a message to website B, then it is likely that A uses Tor to browse B. This attack is out of reach for individuals, but some nation states have the capacity to do so.

As MIT associate professor Nickolai Zeldovich, whose group created Vuvuzela, said: "Tor operates under the assumption that there's not a global adversary that's paying attention to every single link in the world. Maybe these days this is not a good assumption."

Hiding activity as well as metadata

Anonymity through obscurity. Credit: Guy Mayer, CC BY-NC-ND

To overcome Tor's shortcomings, other anonymising software approaches have been proposed, such as Riposte from Stanford University and Dissent from Yale. While they fix Tor's flaws, they are not able to support the sort of usage and number of concurrent users that Tor can, which limits their usefulness.

Vuvuzela is both immune to traffic analysis and other forms of attack, and can support a large number of simultaneous active users. Like Tor, Vuvuzela works by encrypting as much metadata as possible, but (like its namesake) it also adds a lot of noise – fake messages with which to confuse attackers. As they are indistinguishable from genuine messages, this drowns out patterns of genuine communication that might otherwise compromise a user's anonymity.

Unlike Tor, Vuvuzela sends its communication in fixed rounds. Clients cannot send and receive messages at any time, instead on each round a user can only send and receive one message. This obscures the precise timing of messages between sender and receiver, keeping this detail from attackers.

Another difference is how the messages travel. Tor messages pass from sender to receiver in a sequence of hops, while Vuvuzela uses a dead-drop system, where the sender leaves the message at a randomly chosen memory location on one of the Vuvuzela servers, and during a later round the recipient picks up the message.

All messages sent by Vuvuzela messages are the same size, achieved by splitting messages that are too large and padding messages that are too small. This prevents attackers from using message size to compromise anonymity by giving away clues as to what sort of communication is being sent.

As a result, Vuvuzela is the first anonymising privacy system that is

resistant to large-scale network traffic analysis attacks, and which can also sustain millions of active users sending tens of thousands of messages per second.

MIT's software is brand new and still experimental, and cannot yet be considered as a replacement for Tor. It hasn't yet undergone extensive testing through attacks aimed at its theoretical design, and implementation. Crucially, unlike Tor Vuvuzela cannot yet be used for convenient web browsing, nor is it suitable for real-time chat as it is currently quite slow. However, it holds a lot of promise, and may evolve into a viable Tor successor in the future.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation

Citation: Vuvuzela, a next-generation anonymity tool that protects users by adding NOISE (2015, December 18) retrieved 20 April 2024 from https://phys.org/news/2015-12-vuvuzela-next-generation-anonymity-tool-users.html