# How a wall of lamps in an office lobby supports randomness

14 November 2017, by Nancy Owano

Lava lamps in the Cloudflare lobby Credit: Courtesy of @mahtin

(Tech Xplore)—Lava lamps are well known for mood-enhancing functions in living rooms, after-hours cubicles, or anywhere else where humans prefer to dream while wide awake. For a security company with headquarters in San Francisco, however, they serve another key function. They help keep the Internet safe.

A video feed of this wall is used to generate entropy that is made available to their production fleet. The lamps, said the company, provide an unpredictable input to the camera aimed at the wall.

Cloudflare, to be exact, uses them as such.

The lava lamps are used to help generate encryption keys for Internet security—the randomness of the "bubbles" emitted by these lava lamps help generate the encryption keys.

With over 6 million websites using Cloudflare, the company tells its story of having started as a simple application to find the source of email spam. From there it grew into a service that (1) protects websites from attacks and (2) optimizes performance.

"Computers aren't very good at picking random numbers," a presenter in a video about the company, asserts. "Every part of the computer is designed too be is predictable and follow logical patterns."

Put the same numbers in—and get the same numbers out, which is a problem, as safety relies on random numbers.

The presenter is Tom Scott who stands at headquarters of Cloudflare in San Francisco, seen in front of a wall lined with red, blue, pink and green lava lamps.

Actually, the display has a name, the Entropy Wall. "They're used to generate random numbers and keep a good bit of the internet secure," said the video notes.

Cloudflare's Joshua Liebow-Feeser said, "The wall of lava lamps in the office lobby provides a source of true entropy."

The system, LavaRand, serves the purpose of providing an additional entropy source to their production machines.

Paul Lilly in *HotHardware* wrote, "By using lava lamps, Cloudflare has created an additional entropy source with numbers that are based on the flow of the liquid, which is 'very unpredictable.'"

Called LavaRand, the lava lamp system serves as a secondary source for Cloudflare's production servers.

Tyler Lee in *Ubergizmo*: "unlike passwords that can sometimes be guessed, it would be close to impossible to try and predict the pattern that this wall of lava lamps generates."

Liebow-Feeser said, in the lobby, "a camera is pointed at the wall. It obtains entropy from both the visual input from the lava lamps and also from random noise in the individual photoreceptors."

The *Daily Mail* walked readers through what takes place. Images change based on factors such as the movement of the lava, anyone walking by, and shifting daylight – all helping the firm turn data into random numbers.

The footage from the cameras is turned into a stream of random bytes.

Nonetheless, Cloudflare has LavaRand in perspective:

"Hopefully we'll never need LavaRand," according to a blog. "Hopefully, the primary entropy sources used by our production machines will remain secure, and LavaRand will serve little purpose beyond adding some flair to our office. But if it turns out that we're wrong, and that our randomness sources in production are actually flawed, then hopefully LavaRand will be our hedge, making it just a little bit harder to hack Cloudflare."

Liebow-Feeser provides a back story:

"At Cloudflare, we have thousands of computers in data centers all around the world, and each one of these computers needs cryptographic randomness. Historically, they got that randomness using the default mechanism made available by the operating system that we run on them, Linux.

"But being good cryptographers, we're always trying to hedge our bets. We wanted a system to ensure that even if the default mechanism for acquiring randomness was flawed, we'd still be secure. That's how we came up with LavaRand."

**More information:** blog.cloudflare.com/lavarand-i … y-technical-details/


APA citation: How a wall of lamps in an office lobby supports randomness (2017, November 14) retrieved 21 February 2018 from https://techxplore.com/news/2017-11-wall-lamps-office-lobby-randomness.html