The internet is still actually controlled by 14 people who hold 7 secret keys

- Julie Bort
- Oct. 21, 2016, 1:56 PM

It sounds like something out of a Dan Brown book, but it isn't: The whole internet is protected by seven highly protected keys in the hands of 14 people.

And in a few days, they will hold a historic ritual known as the Root Signing Ceremony.

On Friday morning, the world got a good reminder about the importance of the organization these people belong to.

A good chunk of the internet went down for a while when hackers managed to throw so much traffic at a company called Dyn that Dyn's servers couldn't take it.

Dyn is a major provider of something called a Domain Name System, which translates web addresses such as businessinsider.com (easier for humans to remember) into the numerical IP addresses that computers use to identify web pages.

Dyn is just one DNS provider. And while hackers never gained control of its network, successfully taking it offline for even just a few hours via a distributed denial of service attack shows how much the internet relies on DNS. This attack briefly brought down sites like Business Insider, Amazon, Twitter, Github, Spotify, and many others.

Upshot: If you control all of DNS, you can control all of the internet

DNS at its highest levels is secured by a handful of people around the world, known crypto officers.

Every three months since 2010, some — but typically not all — of these people gather to conduct a highly secure ritual known as a key ceremony, where the keys to the internet's metaphorical master lock are verified and updated.

The people conducting the ceremony are part of an organization called the Internet Corporation for Assigned Names and Numbers. ICANN is responsible for assigning numerical internet addresses to websites and computers.

If someone were to gain control of ICANN's database, that person would pretty much control the internet. For instance, the person could send people to fake bank websites instead of real bank websites.

To protect DNS, ICANN came up with a way of securing it without entrusting too much control to any one person. It selected seven people as key holders and gave each one an actual key to the internet. It selected seven more people as backup key holders — 14 people in all. The ceremony requires at least three of them, and their keys, attend, because three keys are needed to unlock the equipment that protects DNS.

A highly scripted ritual

The physical keys unlock safe deposit boxes. Inside those boxes are smart key cards. It takes multiple keys to gain access to the device that generates the internet's master key.

That master key is really some computer code known as a root key-signing key. It is a password of sorts that can access the master ICANN database. This key generates more keys that trickle down to protect various bits and pieces of the internet, in various places, used by different internet security organizations.

The security surrounding the ceremonies before and after is intense. It involves participants passing through a series of locked doors using key codes and hand scanners until they enter a room so secure that no electronic communications can escape it. Inside the room, the crypto officers assemble along with other ICANN officials and typically some guests and observers.

The whole event is heavily scripted, meticulously recorded, and audited. The exact steps of the ceremony are mapped out in advance and distributed to the participants so that if any deviation occurs the whole room will know.

The group conducts the ceremony, as scripted, then each person files out of the room one by one. They've been known to go to a local restaurant and celebrate after that.

But as secure as all of this is, the internet is an open piece of technology not owned by any single entity. The internet was invented in the US, but the US relinquished its decades of stewardship of DNS earlier this month. ICANN is officially in charge.

Keenly aware of its international role and the worldwide trust placed on it, ICANN lets anyone monitor this ceremony, providing a live stream over the internet. It also publishes the scripts for each ceremony.

On October 27, ICANN will hold another ceremony — and this one will be historic, too. For the first time, it will change out the master key itself. Technically speaking, it will change the "key pair" upon which all DNS security is built, known as the Root Zone Signing Key.

"If you had this key and were able to, for example, generate your own version of the root zone, you would be in the position to redirect a tremendous amount of traffic," Matt Larson, vice president of research at ICANN, recently told Motherboard's Joseph Cox.