Technical Argument and Explanation / Visualisation

Amartya Vadlamani

October 11, 2016

1 Quoted article

1.1 URL and Title

http://uclengins.org/external/the-cryptographic-key-that-secures-the-web-is-being-changed-for-the-first-time/view/

The Cryptographic Key That Secures the Web Is Being Changed for the First Time

1.2 Article Body

Soon, one of the most important cryptographic key pairs on the internet will be changed for the first time.

The Internet Corporation for Assigned Names and Numbers (ICANN), the US-based non-profit responsible for various internet infrastructure tasks, will change the key pair that creates the first link in a long chain of cryptographic trust that lies underneath the Domain Name System, or DNS, the "phone book" of the internet.

This key ensures that when web users try to visit a website, they get sent to the correct address. Without it, many internet users could be directed to imposter sites crafted by hackers, such as phishing websites designed to steal information.

ICANN wants to be very transparent in the operation of this key because it's important that the community trusts it, Matt Larson, vice president of research at ICANN, told Motherboard in a phone call.

Matt Larson of ICANN. Image: Kim Davies/Flickr

DNS translates easy-to-remember domain namessuch as Google.cominto their numerical IP addresses, so computers can visit them. But DNS was never built with security in mind. The domain name system was designed when the internet was a friendlier place, and there wasn't much thought of security put into it, Larson said.

As a result, a particular problem has been something called DNS cache poisoning or DNS spoofing, where a server doing the phone book-like lookups is forced to return an incorrect IP address, resulting in traffic being diverted somewhere else, such as a malicious site controlled by a hacker.

To deal with this problem, many domains use DNS Security Extensions (DNSSEC). With DNSSEC, crypto keys authenticate that DNS data is coming from the correct place. If something dodgy has happened along the way and the signatures don't line up, your browser will just return an error instead of being sent to the wrong website. DNSSEC doesn't encrypt data on the sitethat's a job for protocols such as SSL or TLSbut lets you know whether the site you're trying to visit is legitimate.

In 2010, ICANN, along with other organisations, introduced DNSSEC to protect the internets top DNS layer, the DNS root zone.

A hierarchy of keys governs the process of DNSSEC authentication, with different bodies responsible for each stage of the system. The top-level root zone, managed by ICANN, is followed by the operators of different top level domains such as .com, and then those managing individual domains, such as MyWebsite.com.

"If you had this key ... You would be in the position to redirect a tremendous amount of traffic"

Each organisation in this structure has its own keys for making signatures, and must sign the key of the entity below it. So for MyWebsite.com, .com will sign MyWebsite.com's key, and the root will sign .com's key. When visiting a website, this information is checked almost instantaneously, before your computer loads up the correct site. Not everyone uses DNSSEC, but adoption has increased over the years: Comcast turned it on for its customers in 2012, and in 2013, Googles own DNS service started to fully support DNSSEC.

The key pair at the top of this chain, or the Root Zone Signing Key, is what ICANN is changing for the first time.

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, Larson said.

We want to roll the key because it's good cryptographic hygiene, he added.

In the same way that it might be a good idea to change your password in case it was swept up in a data breach, changing keys every so often is a standard security practice.

There is a logical possibility that somebody has cracked it and we dont know, Andrew Sullivan, chair of the Internet Architecture Board, a group that oversees organisations involved in the evolution of the internet, told Motherboard in a phone call. He stressed, however, that there is no reason to believe the key has been compromised.

Indeed, ICANN incorporates some extraordinary security measures, and considers its potential threats as everything up to nation states. For its quarterly ceremonies, so-called crypto officers from all over the world congregate in one of the key management facilities, after passing layers of physical and digital security.

Another reason for the key switch is that it is going to increase in size, from 1024 bits up to 2048. As time goes on, and computing power increases, the chance of someone cracking the key, although still low, increases.

It's important to get a larger key for the root, and I don't want to see anything delay that, Dan Kaminsky, a renowned security researcher who carried out much of the early work into DNS security, told Motherboard in an email.

ICANN wants to make the change during a period of calm, rather than having to act quickly if the key was compromised.

We want to do this process when things are normal; when there's not any kind of emergency, Larson said. This way, if an actor does manage to get the key somehow later, at least ICANN will have a better idea of how the process works.

This October, in one hyper-secure key management facility on the US east coast, ICANN will generate a new cryptographic key pair. One half of that pair is private, and will be kept by ICANN; the other is public. Internet service providers, hardware manufacturers, and Linux developers need the public key part for their software to connect to sites properly.

In the first quarter of 2017, two employees will then take a copy of the encrypted key files on a smartcard over to another facility on the west coast, using regular commercial transport. Eventually, the public part of the key pair will be distributed to other organisations.

In all, the whole switchover will take around two years from start to finish. Larson said that the new key will appear in the DNS for first time on July 11, 2017. In October 2017, the new key will be used for making signatures.

Getting the word out in time is one of the main concerns. Although many larger organisations will have already been monitoring the looming key change for some time, Sullivan said theres a chance that a piece of hardware left on a shelf between now and the key change, such as a router or firewall appliance, may miss the switchover and require a manual update.

Talking to media is one way of spreading the message, but being very public about the key change also serves another purpose that is very much fundamental to the internets infrastructure generally: trust.

Because the internet is a network of networks and it's all voluntary, people have to believe they are getting some value out of this, otherwise they just won't use it, Sullivan said.

DNSSEC and other forms of authentication may seem like totally technological solutions. But at bottom, they are also systems resting on the fragility of human belief.

Ultimately, no one can know with absolute certainty whether the ICANN key has been compromised or not.

Trust is an ephemeral thing, said Larson from ICANN.

Correction: The Root Zone Signing Key was originally described as an "encryption key." It is a cryptographic key pair, but not an encryption key. The headline of this story has been amended; we regret the error.

2 Answers to questions

What is the status quo? The "1024 bit" signing keypair is used as the root keypair for the DNS tree of trust.

What is the problem? It needs to be rotated and upgraded to a "2048 bit" keypair

What are the competing solutions? ... No competing solutions discussed as one used already

How does the proposed solution work? It changes the key like changing the password on an account to a longer one

How well does it work? Apparently good enough for the ICANN

What else do I need to know? Not much