First Results in Analyzing the Certificate Transparency Ecosystem

Karoline Busse, Christian Tiefenau, Matthew Smith
Usable Security and Privacy Group
Rheinische Friedrich-Wilhelms-Universität Bonn

What is Certificate Transparency?

The Certificate Transparency (CT) technology makes rogue CAs visible and greatly reduces the time in which a misissued certificate can be used unnoticed. During the issuance process, a certificate must be submitted to at least one publicly auditable, append-only **Log** server. When establishing a secure connection, the server is obliged to provide a list of Logs in which the certificate is published, so the client can check its validity. In addition, domain owners can run **Monitors** that periodically query selected Logs for illegitimately issued certificates for their sites.

What is the CT Observatory?

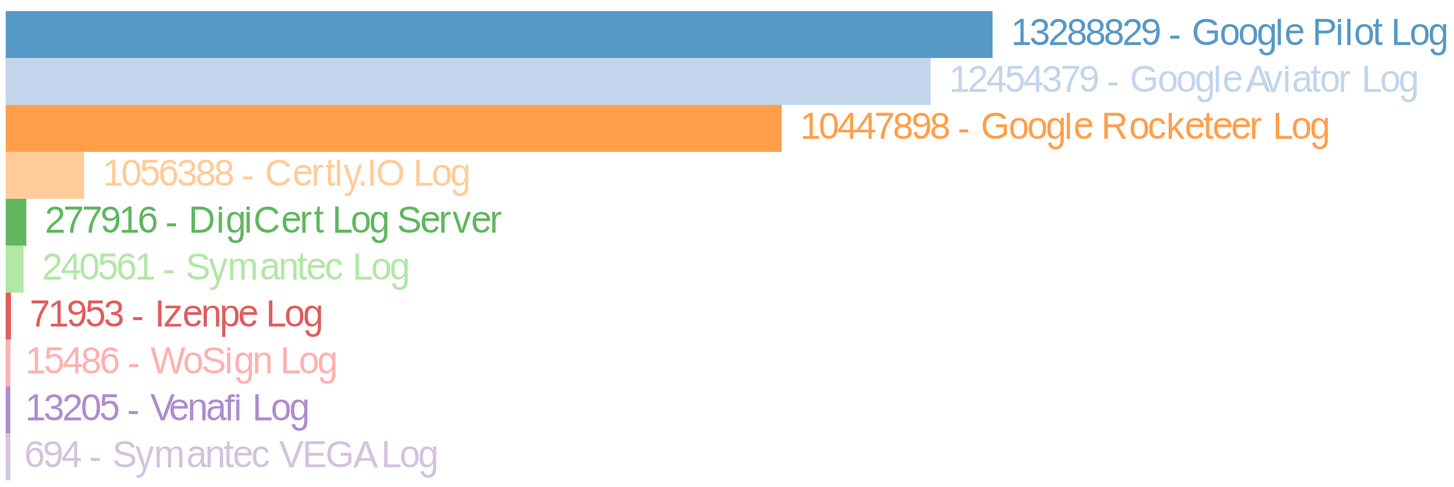
The observatory is an internet-wide monitor that runs additional analyses about the gathered Log data. So far, 10 logs have been set up across 7 organizations, collecting a total of 13245364 certificates of which 6385173 are currently valid. This corresponds to 14.44 % of all certificates used for HTTPS connections in the IPv4 part of the internet (as provided by Censys).

Future Plans

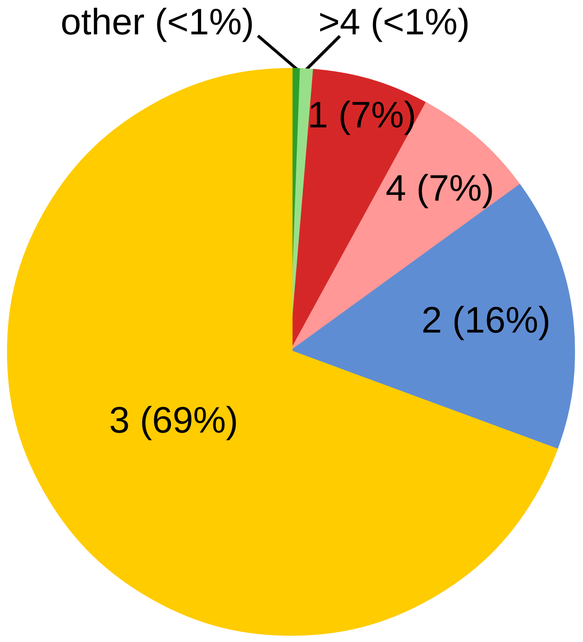
A major task for the Observatory is to detect suspicious behavior in the Log data, including:

- Switching a CA
- Key change
- Same certificate with interesting new extensions
- First wildcard certificate for a domain
- New certificates using weaker crypto than existing ones

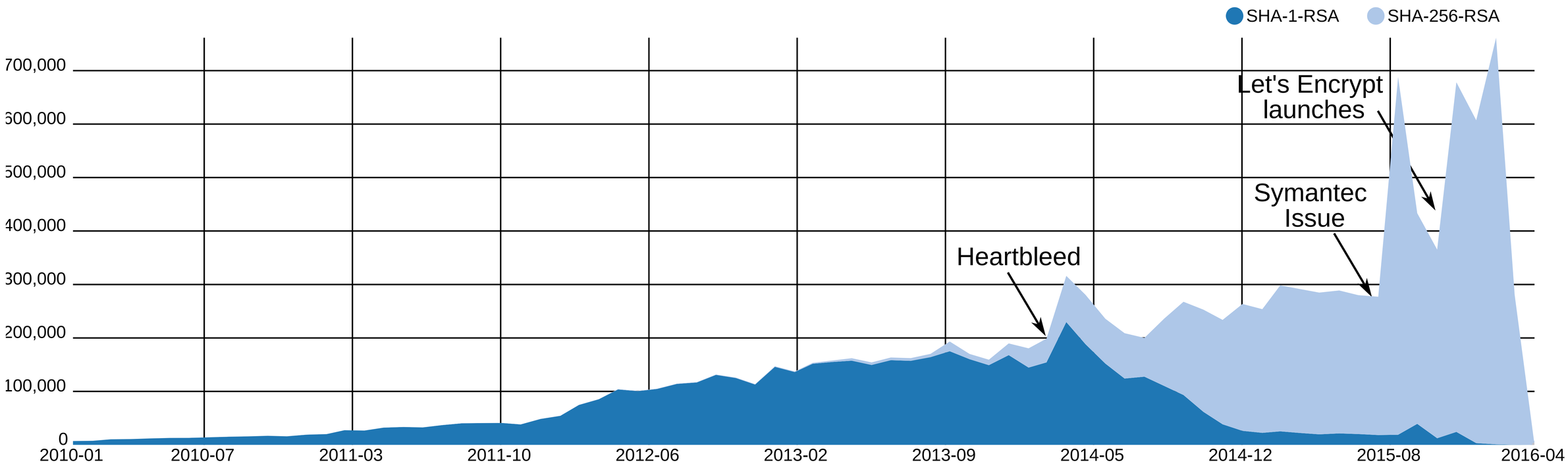
In addition, we want to provide an in-depth analysis of historical certificate data for future work that is accessible for researchers and other interested entities. The extension of a notification for site owners in case of suspicious behavior is also planned. This could be realized e.g. through email notification or by providing a Nagios module.
The Observatory is currently running on our server and already collecting certificates. It will be made accessible to the public in the near future.



The ten public Logs listed on www.certificate-transparency.org and their respective number of incorporated certificates



Number of logs a single certificate is incorporated in



Signature algorithms in newly issued certificates (notBefore date), by month.

This project is a part of the BMBF-funded joint research on „BDSec – Big Data Security“

Powered by: Django ● crt.sh ● d3.js ● jQuery ● Bootstrap ● Docker

https://github.com/USECAP/ct-infrastructure