Abstract title:
The ICSI Notary: Lessons and Insights from a Large-Scale Study of the SSL/TLS Ecosystem

Technology space:
Transparency and alternative certification, distribution or confirmation of key information

Authors:
Bernhard Amann (International Computer Science Institute) Matthias Vallentin (UC Berkeley) Robin Sommer (International Computer Science Institute, Lawrence Berkeley National Laboratory)

Abstract:
We present our experiences and results from an extensive, ongoing live measurement effort aimed at understanding the global SSL/TLS ecosystem from an unprecedented vantage point. For about a year now, we have been passively monitoring all SSL sessions at the Internet uplinks of 7 large-scale institutions, observing activity of more than 300,000 unique users and more than 1 billion SSL/TLS sessions each month. We are currently studying this data from a number of different perspectives, with a particular focus on changes to the global CA trust hierarchy over time. As our data set provides a comprehensive, up-to-date view of SSL certificates seen in the wild, we believe that conceptually it resembles what proposed efforts such as Certificate Transparency aim to institutionalize in the future. As such, we are leveraging our collection to study opportunities but also hurdles that CT will encounter in practice due to the real-world pecularities that come naturally with such a large-scale decentralized ecosystem. We are furthermore operating a DNS-based notary service as a community resource, which provides daily usage information about individual certificates in our data set to support endusers' trust assessments.

For more information see http://notary.icsi.berkeley.edu.

With kind regards,
Bernhard Amann