A Summary of 'A Longitudinal, End-to-End View of the DNSSEC Ecosystem'

Ally Smith

due April 28, 2022

Much like some of the other papers we have read in this class, the sheer magnitude of this study is impressive. However, something that sets this paper apart from the rest is the extreme levels of misuse of the DNSSEC infrastructure. With 31% of domains failing to publish the relevant information, to only 12% of resolvers attempting to validate the records they receive, this is far greater levels of noncompliance than in other papers. Overall, the approach that they took in their research was very standard for a project like this. They were able to survey large amounts of nodes, and checked which of those they found were reporting that they supported DNSSEC, and which, out of those, actually implemented it in a way that granted practical improvements to security. I think this could possibly tie in with the first research paper, in that it is possible that the maintainers of these keys are simply ignorant to the proper ways to use DNSSEC, and the documentation around it is not clear enough to users for the layman to set it up appropriately. Another interesting finding from this paper was that certain domains share keys for efficiency reasons. While this is an intentional decision made by the key holders, the paper recommends against this as it 'substantially increases security risk.'