Contribution ID : **23** Type : **Standard Presentation**

NSEC5: Updated specification and implementation results

Monday, 15 May 2017 09:45 (30)

NSEC5 is a proposed enhancement to DNSSEC that provably prevents zone enumeration. It does this by replacing the hashes used in NSEC3 with hashes computed by a verifiable random function (VRF), and requiring authoritative servers to perform a small amount of online cryptography for negative responses. This talk will give an overview of the latest NSEC5 protocol specification, and describe the results of implementing it and evaluating its performance.

Summary

Talk Duration

30 Minutes

Primary author(s) : HUQUE, Shumon (Salesforce)

Co-author(s) : LAWRENCE, David (Akamai Technologies); VČELÁK, Jan (NS1)

Presenter(s) : LAWRENCE, David (Akamai Technologies); VČELÁK, Jan (NS1); HUQUE, Shumon (Salesforce)

Session Classification : Public Workshop: DNSSEC

Track Classification : Public Workshop