Design and Performance Analysis of Optimization Algorithms for Efficient Cryptographic Processing in Secure Internet Routing Protocol

Sriram, Vinay

This project proposes new dynamic optimization algorithms that provide significant cache management enhancements over the known three basic algorithms for signature verifications to improve efficiency in secure internet routing protocol in BGPSEC (Border Gateway Protocol with SECurity), a standardization protocol currently under consideration by the Internet Engineering Task Force. My findings (1) enable router manufacturers to appropriately size the CPU to be used in route-processors, (2) recommend an optimization algorithm for implementation in BGPSEC routers, (3) show router table convergence can be sped up without increasing the cost of the CPU for route-processing. These three elements are key hurdles for the implementation of BGPSEC; due to the cryptographic processing required, BGPSEC imposes a significantly greater workload on route processors in currently used BGP routers. In 2012, I evaluated the basic optimization algorithms for signature verifications in BGPSEC and their performance in terms of processor cost and energy consumption. This year I designed new optimization algorithms and using detailed simulations and analytical modeling studied the performance of the optimizations to quantify relative and absolute efficiencies measured by peak-second count of signature verifications, a task which dominates BGPSEC-related processing in the core-facing routers in the Internet. The best of our proposed new algorithms achieves approximately an order of magnitude reduction over the unoptimized method in terms of the peak-second count of signature verifications. Our results are expected to help equip router manufacturers to implement BGPSEC in a cost effective and efficient way.

Awards Won:
Fourth Award of $500