Title:
Verifying Keys through Publicity and Communities of Trust: Quantifying Off-Axis Corroboration

Authors:
Eric Osterweil Verisign Labs eosterweil@verisign.com Dan Massey Colorado State University massey@cs.colostate.edu Danny McPherson Verisign Labs dmcpherson@verisign.com Lixia Zhang UCLA lixia@cs.ucla.edu

Abstract:
The DNS Security Extensions (DNSSEC) arguably make DNS the first core Internet system to be protected using public key cryptography. The success of DNSSEC not only protects the DNS, but has generated interest in using this secured global database for new services such as those proposed by the IETF DANE working group. However, continued success is only possible if several important operational issues can be addressed. For example, .gov and .fr have already suffered misconfigurations where DNS continued to function properly, but DNSSEC failed (thus orphaning their entire subtrees in DNSSEC). Internet-scale verification systems must tolerate this type of chaos, but what kind of verification can one derive from dynamism like this?

In this paper, we propose to achieve robust verification with a new theoretical model, called Public Data, which treats operational deployments as Communities of Trust (CoTs) and makes them the verification substrate. Using a realization of the above idea, called Vantages, we quantitatively show that using a reasonable DNSSEC deployment model and a typical choice of a CoT, an adversary would need to "compromise up to 90% of the Internet" before having even a 10% chance of spoofing a DNSKEY. Further, a limited trial deployment of Vantages, Public Data outperformed the verifiability of DNSSEC and properly validated data up to 99.5% of the time.