Cryptology ePrint Archive: Report 2013/017

Provable Security of S-BGP and other Path Vector Protocols: Model, Analysis and Extensions

Alexandra Boldyreva and Robert Lychev

Abstract: This paper provides the provable-security treatment of path vector routing protocols. We first design a security definition for routing path vector protocols by studying, generalizing, and formalizing numerous known threats. Our model incorporates three major security goals. It is quite strong, yet simple to use. We prove by reduction that S-BGP satisfies two out of the security model's three goals, assuming the underlying signature scheme is secure. Under the same assumption, we next show how the protocol can be modified to meet all three security goals simultaneously. We also analyze SoBGP and show that it fails to meet two security goals. Finally, we study security of partial PKI deployment of path vector protocols when not all nodes have public keys. We investigate the possibilities of relaxing the PKI requirement and relying on non-cryptographic physical security of networks that use the protocol in order to achieve possibly weaker, but still well-defined, notions of security. We also present the necessary and sufficient conditions to achieve full security in the partial PKI deployment scenario. We believe our conclusions will prove useful for protocol developers, standards bodies and government agencies.

Category / Keywords: Applications / Secure BGP, routing protocols, path vector protocols, protocol verification, provable security

Publication Info: A preliminary version of this paper appears in ACM Conference on Computer and Communications Security 2012.

Date: received 10 Jan 2013, last revised 10 Jan 2013

Contact author: robert lychev at gatech edu