Cryptographically Secure Detection of Mirror Worlds

Stoyanov, Hristo

The Resource Public Key Infrastructure (RPKI) has been introduced as a way of authorizing Border Gateway Protocol (BGP) route announcements. The highly centralized structure of the RPKI provides security guarantees against external threats, e.g. prefix hijacking, but allows for the unilateral revocation of allocated resources. Recent efforts propose changes to the RPKI to create accountability of such unilateral actions. The project under consideration continues these efforts by providing a mechanism for ensuring global consistency. We solve the global consistency problem by constructing a k-connected graph containing all 2-party audits that the honest Autonomous Systems must perform to ensure that no mirror worlds exist. This mechanism can lead to wider adoption to the RPKI.

Awards Won: