
Some Steps towards Improving the Resiliency of
the Internet Routing System:

The Role of a Registry Certificate Authority

Geoff Huston
Telstra

Vulnerability

- Internet hosts are the subject of constant malicious attack
 - The DNS is the subject of continual attempts to subvert its correct operation
 - Widespread malicious attacks on the Internet's routing system are only a matter of time...
 - Attacks on the operation of the routing protocols
 - Attacks on weaknesses in the administrative systems used to manage routing configurations
-

Injecting Routes

- Administrative system
 - Customer passes prefix information to provider
 - Provider performs registry-based check on the relationship between the customer and the requested prefix
 - Passes the prefix and the customer details to the router config system
 - Pass prefix details to route neighbours
 - Router configuration
 - Entry of static routes / route filter into config database
 - Periodic generation of router configs from database
-

Administrative Weaknesses

- Link between ISP's records of customer and registry address records can be incomplete or inconsistent
 - ISPs want to do the right thing by the customer and by their own business
 - Rapid service response
 - Respond positively to route requests
 - Spend minimal administrative overhead in operating the system
-

Potential Role of Key Certificates

- Registry records include public key for each allocated prefix
 - Customer controls private key
 - Administrative requests to ISP signed with private key of the corresponding prefix
 - ISP uses registry public key to validate customer request
 - ISP passes signed request to neighbors who will receive the re-advertised route, signing the neighbor request with the ISP's private key
-

Commentary

- Does not eliminate need for secure routing protocols
 - Allows ISPs to use a trusted third party (Registry) to validate route requests:
 - Quickly
 - With minimal manual processing overhead
 - Accurately (*)
 - Any customer who leaks a private key is beyond help!
 - Details and procedures need to be refined...
-