Update Critical Infrastructure to Include PKI

Tom Paseka

APNIC-34, 30 August Phnom Penh

Introduction

- Public Key Infrastructure is critical for online security (SSL).
- Online Certificate Status Protocol (OSCP) and Certificate Revocation List (CRL), RFC-2560 and RFC-3280 respectively.
- Validate X.509 SSL Certificates.

Current problem

- Current policy doesn’t define PKI as critical infrastructure.
- Resources managed through existing allocations

Other RIRs

- Same position in other RIRs
- Proposal will be submitted in due course.

Proposal

- Amend APNIC-124 / Policies for IPv4 address space management in the Asia Pacific region:
  - Point 3.5 to include Public Key Infrastructure
- Amend APNIC-089 / IPv6 address allocation and assignment policy
  - Point 5.9.3 to include Public Key Infrastructure

Benefits/disadvantages

- Benefits:
  - Public Key Infrastructure providers will have a block of defined address space for PKI.
  - Access to allocations
- Disadvantages:
  - Increased address allocation
  - More member and resource allocations requests
  - More workload on APNIC

Summary

- Include PKI as Critical Infrastructure
  - Critical for Internet Security

- Protocol Information:

  X.509 Internet Public Key Infrastructure
  Online Certificate Status Protocol – OSCP
  http://tools.ietf.org/html/rfc2560

  Internet X.509 Public Key Infrastructure
  Certificate and Certificate Revocation List (CRL) Profile
  http://tools.ietf.org/html/rfc3280