



ASIA-PACIFIC TELECOMMUNITY

5th APT CYBERSECURITY FORUM (CSF-5)

26-28 May 2014, Ulaanbaatar, Mongolia

**Document
CSF-5/INP-13**

19 May 2014

Mr. Adli Wahid, APNIC

OPPORTUNITIES AND CHALLENGES IN CYBERSECURITY

Contact :

Mr. Adli Wahid,
APNIC

Tel: +61411022391 (mobile) +61731583100
Email: adli@apnic.net

Cyber Security Opportunities and Challenges

Adli Wahid

Security Specialist, APNIC

5th APT Cyber Security Forum, (27-29th May 2014)

APNIC

Issue Date:

Revision:



Agenda

1. Overview of APNIC

2. Opportunities and Challenges

- Source Address Validation (BCP38)
- Securing the Internet with Resource Certification
- Effective Incident Response & Handling (Whois Database)
- Awareness and Education

3. The Way Forward

Overview

Serving APNIC Members

Supporting Internet development
in the Asia Pacific region

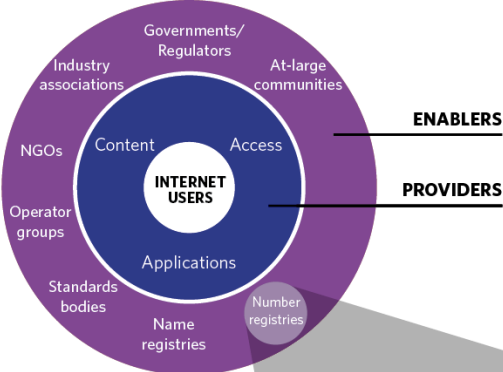
Collaborating with the Internet
community

APNIC's Vision:
*“A global, open,
stable, and secure
Internet that
serves the entire
Asia Pacific
community”*

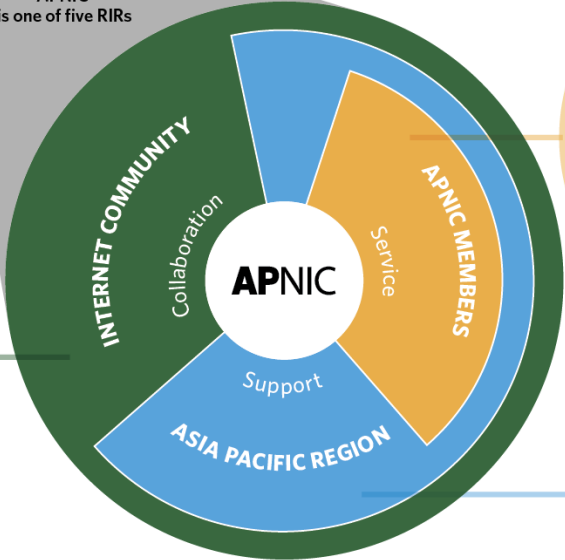
APNIC's Mission

- **Function as the RIR** for the Asia Pacific, in the **service** of the community of Members and others
- Provide Internet registry services to the highest possible standards of **trust, neutrality, and accuracy**
- Provide **information, training, and supporting services** to assist the community in building and managing the Internet
- Support **critical Internet infrastructure** to assist in creating and maintaining a robust Internet environment
- Provide **leadership and advocacy** in support of its vision and the community
- Facilitate **regional Internet development** as needed throughout the APNIC community

APNIC in the Internet ecosystem



APNIC is one of five RIRs



Resource distribution

- IP addresses
- AS numbers

Registration services

- reverse DNS
- Internet routing registry
- resource certification
- whois registry

Policy development

Capacity building

- training
- workshops
- conferences
- fellowships
- grants

Infrastructure

- root servers
- IXPs
- engineering assistance

- Original research
- Data collection and measurements
- Publications
- Local/regional/global events
- Government outreach
- Intergovernmental & technical organizations collaboration
- Internet security

Strategic Engagement

Technical community

- NOGs, NIR OPMs, I*, CERTs, ISOC Chapters, PACINET, PICISOC, PTC

Governmental

- APEC-TEL 47 and 48, ITU WTPF, APT, WSIS+10, ITU Connect Asia Pacific Summit, ITU Telecom World 2013, APEC TEL 49, NETmundial

IGF

- National IGFs (Nethui, auIGF), APriIGF
- Bali IGF - significant support given for fundraising and logistics

Opportunities & Challenges

Opportunities & Challenges

- Government institutions, CERTs, Law Enforcement Agencies and stakeholders have been collaborating all along
- What else needs to be done?
- What are the challenges?

Source Address Validation

- Problem
 - Network providers allow traffic from IP addresses that they do not hold
 - As a result it is trivial to spoof IP addresses
 - This enabled attacks such as DDoS Amplification
- Recipe for Amplification Attacks
 - Network that allows source IP spoofing
 - Network services that respond to non-customers requests
- This is not new
 - Best Current Practice 38 has been around since 2000 (RFC 2827)
 - Also known as Network Ingress Filtering

Resource Certification with RPKI

- Resource Public Key Infrastructure
 - Security framework to verify association between specific IP address blocks or Autonomous System (AS) numbers and the holders of the resources
 - Using Digital Certificates and Public Key Cryptography
- Essential because
 - Improve security of inter-domain routing. Currently based on mutual trust
 - Able to prove authoritatively prove who owns an IP address block and what AS may announce it

Resource Certification Benefits

- What does it address?
 - Prevent Mis-origination or “Route Hijacking”
 - When an entity participating in Internet Routing announces a prefix without authorisation (either mistake or malicious intention)
- Benefits
 - Routing Information corresponds to properly delegated address resources
 - Resource Certification gives resource holders proof that they hold certain resources
 - Resource holders can attest to those resources when distributing them
 - Resource certification a highly robust means of preventing the injection of false information into the Internet routing system.

Resource Certification with RPKI

- Role of APNIC
 - Act as Certificate Authority, attest that the certificate belong to the identified party
 - Issues RPKI certificates to APNIC members
 - This has been rolled out since 2013

WHOIS Database – Improving Incident Response & Handling

- Security Incidents happen and timely response is critical
- The IRT (Incident Response Team) object requires resource holders to provide contact information
- There are opportunities to
 - Enhance Incident Response & Handling Capabilities
 - Provide additional information for escalation (i.e. National CSIRT/CERT or relevant agency)
 - Report invalid contact information

Awareness and Education

- Reaching out to operators (resource holders) and relevant stakeholders is important to create awareness and ability to apply best current practices
- Challenges:
 - Cost and availability of subject matter expert
- APNIC provides training at events across the region as well as online
 - <http://training.apnic.net/>
- Topics include
 - BGP, IPv6, DNS-SEC, Network Security and many more

The Way Forward

- Infrastructure security issues are part of the bigger picture and must be addressed
- The full impact of security controls may only be realised if everyone implement them
 - Relevant stakeholders & operators must make things happen
- Awareness and Education activities are at the core of all of the above
- Let's work together!

Thank You!

Adli Wahid

Security Specialist, APNIC

adli@apnic.net

You're Invited!

- APNIC 38: Brisbane, Australia, 9-19 Sep 2014



- APRICOT 2015: Fukuoka, Japan, 24 Feb-6 Mar 2015



THANK YOU



www.facebook.com/APNIC



www.twitter.com/apnic



www.youtube.com/apnicmultimedia



www.flickr.com/apnic



www.weibo.com/APNICrir