# APNIC's role in stability and security

Adam Gosling

Senior Policy Specialist, APNIC

4th APT Cybersecurity Forum, 3 - 5 December 2013

APNIC

# Overview

- Introducing APNIC
- Working with LEAs
- The APNIC Whois Database
- Internet Routing Registry
- DNS Security Extensions
- Resource Public Key Infrastructure

APNIC

# Introducing APNIC

*"A global, open, stable, and secure Internet that serves the entire Asia Pacific community"*

APNIC

# What is APNIC?

- Regional Internet Registry (RIR) for the Asia Pacific region
  - Comprises 56 economies
- Not-for-profit, membership-based organization
- Governed by Member-elected Executive Council (EC)
- Secretariat located in Brisbane, Australia
  - Currently employs around 70 staff


APNIC


RIPE NCC
ARIN
American Registry for Internet Numbers
APNIC
AFRINIC
The Internet Numbers Registry for Africa
10
2002:2012
LACNIC

# APNIC's Vision:

***A global, open, stable, and secure Internet that serves the entire Asia Pacific community.***

How we achieve this:

- Serving Members
- Supporting the Asia Pacific Region
- Collaborating with the Internet Community

# APNIC: What do we do?

- Management and Distribution of Internet Resources
  - IPv4 and IPv6 addresses, AS Numbers
- The APNIC Whois Database
  - Troubleshooting
  - Tracking source of abuse
  - Protecting address space to prevent hijacking
- Manages Reverse DNS delegations
- Supports Internet development
  - Root server deployment & ISIF
- Is an authoritative source of information
  - APNIC Conferences, Technical talks & tutorials
  - APNIC LABs
- Development services
  - Training courses, Workshops and Seminars
- Facilitates the policy development process
  - Via mailing lists, conferences etc.
- Collaboration & Liaison

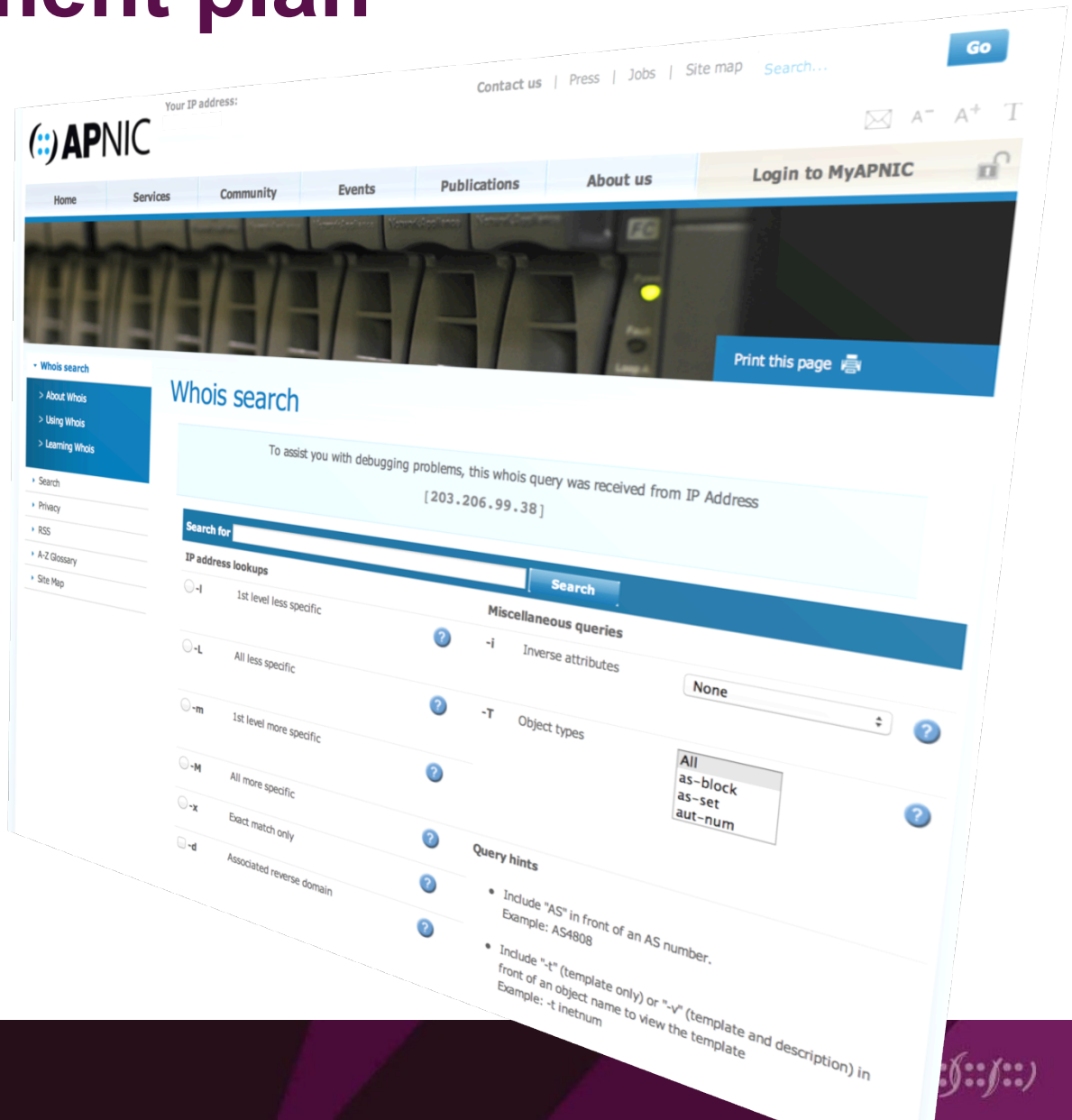
# APNIC and Law Enforcement Agencies

*Law enforcement agencies are an important part of the APNIC community*

APNIC

# LEA engagement plan

- We collaborate, cooperate and work together with LEAs in the community to help keep the Internet open, secure, and stable
- Data from the whois may be a source of information for LEAs, for example, tracking the source of network abuse



# Assisting Law Enforcement Agencies

- Provide training and capacity building to help them to explore the data on the public WHOIS database
  - Training LEA's in collaboration with country-code top level domain name managers in region
- Work to improve accuracy and reliability of
  - The APNIC Whois Database
  - Reverse DNS zone delegations
- We encourage LEAs to participate in the APNIC PDP, so that important issues affecting LEAs are considered
- New security specialist on staff to assist in LEA engagement plan

# The APNIC Whois Database

APNIC

# The APNIC Whois Database

- Holds IP address records within the Asia Pacific region
- Used to track down the source of network abuse
  - IP addresses, ASNs, reverse domains, routing policies
- Identify network contacts from registration records
  - IRT (Incident Response Team) if present
  - Contact persons: “tech-c” or “admin-c”
- Records of network administrators
  - Not individual users
  - Use administrators log files to contact the individual involved

# Whois Object Types

| OBJECT | PURPOSE |
|---|---|
| person | contact persons |
| role | contact groups/roles |
| inetnum | IPv4 addresses |
| Inet6num | IPv6 addresses |
| aut-num | Autonomous System number |
| domain | reverse domains |
| route | prefixes being announced |
| mntner | (maintainer) data protection |
| mnt-irt | Incident Response Team |

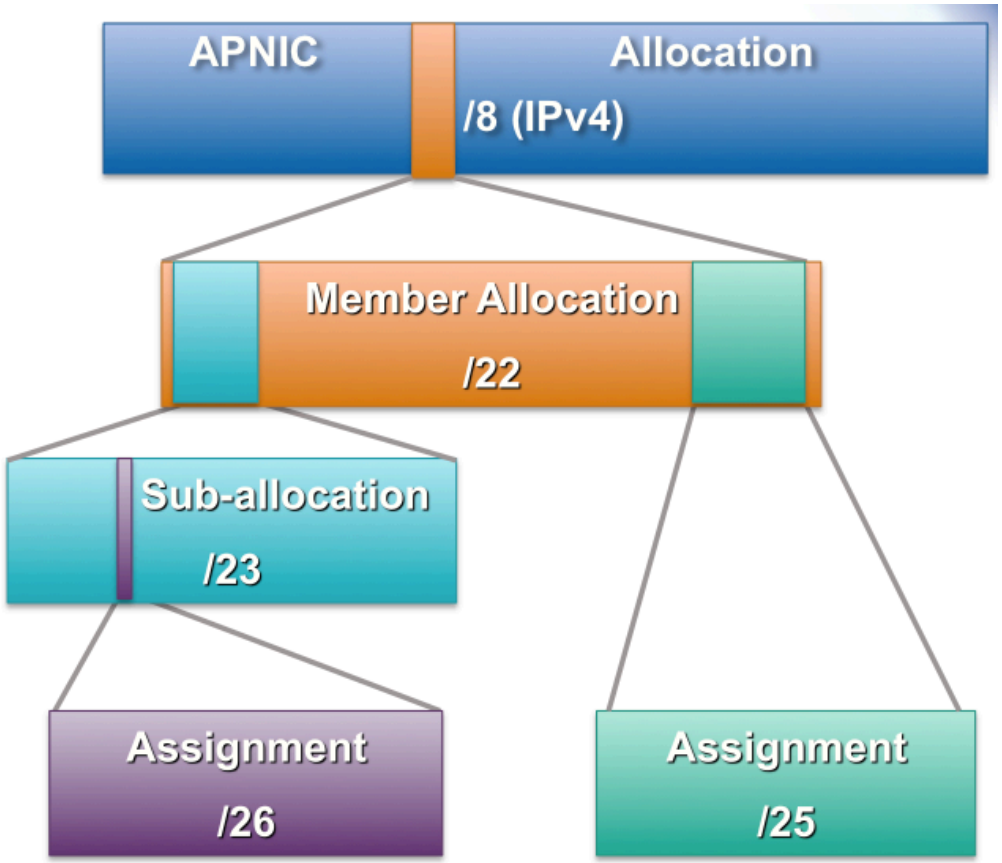
http://www.apnic.net/db/

# Maintainer Hierarchy Diagram

**Allocated to APNIC:**
Maint-by can only be changed by IANA

**Allocated to Member:**
Maint-by can only be changed by APNIC

**Sub-allocated to Customer:**
Maint-by can only be changed by Member



# Resource Registration

- As part of the membership agreement with APNIC, all members are required to register their resources in the APNIC Whois database.
- Members must keep records up to date:
  - Whenever there is a change in contacts
  - When new resources are received
  - When resources are sub-allocated or assigned

# Customer privacy

- Public data
  - Includes portable addresses (inetnum objects), and other objects, for example, route objects
  - Public data: must be visible
- Private data
  - Can include non-portable addresses (inetnum objects)
  - Members have the option to make private data visible
- Customer assignments
  - Can be changed to be public data (public data is an optional choice)

# Efforts in Preventing Network Abuse

- As a registry, APNIC **adopts and applies policies** for it's community which address network abuse. APNIC does not have the capacity to investigate abuse complaints or the legal powers to regulate Internet activity.
- APNIC seeks to raise awareness of the need for **responsible network management in the Asia Pacific**, through training and communication.

# Can APNIC stop abuse?

- No, because…
  - APNIC is not an ISP and does not provide network connectivity to other networks
  - APNIC does not control Internet routing
  - APNIC is not a law enforcement agency
  - APNIC has no industry regulatory power

# Investigation of complaints

- Laws relating to network abuse vary from country to country
- Investigation possibilities
  - Cooperation of the network administrators
  - Law enforcement agencies
    - Local jurisdiction
    - Jurisdiction where the problem originates

# What can you do?

- Use the APNIC Whois Database to obtain network contact information
- APNIC Whois may or may not show specific customer assignments for the addresses in question
  - But will show the ISP holding APNIC space
- Contact the network responsible and also its ISP/upstream
- Contact APNIC for help, advice, training or support
- Community discussions can be raised in the APNIC conferences,  mailing lists, etc.

# Steps we take to improve accuracy

- Member account opening
  - verification of corporate existence with corporate registries or regulators (where possible)
- Membership renewal
  - once a year
  - email to corporate contact, with payment record
  - Internet resources revoked if account not paid or renewed
- Transfer policies
  - encourage registration of resources
  - “value” of Internet resources encourage registration

# What if Whois info is invalid?

- Members (ISPs) are responsible for reporting changes to APNIC
  - Under formal membership agreement
- Report invalid ISP contacts to APNIC
  - http://www.apnic.net/invalidcontact
  - APNIC will contact member and update registration details

# New features

- New and improved features to provide a more stable and reliable service
  - “geoloc” and “language” attributes added to inetnum and inet6num objects
  - New feature to view previous versions of resources and how a specific object was changed over time
- Registration Data Access Protocol (RDAP)
  - Suite of specifications currently under development under the IETF’s Web Extensible Internet Registration Data Service (WEIRDS)
  - Pilot service available to test the RDAP protocol
  - Collaboration with the RIPE NCC

# Internet Routing Registry (IRR)

APNIC

# APNIC Whois Database and the IRR

- APNIC Whois Database
  - Two databases in one
- Public network management database
  - “Whois” information about networks and contact persons
    - IP addresses, AS numbers etc
- Routing registry (RR)
  - Contains routing information
    - Routing policy, routes, filters, peers etc.
  - APNIC RR is part of the global IRR

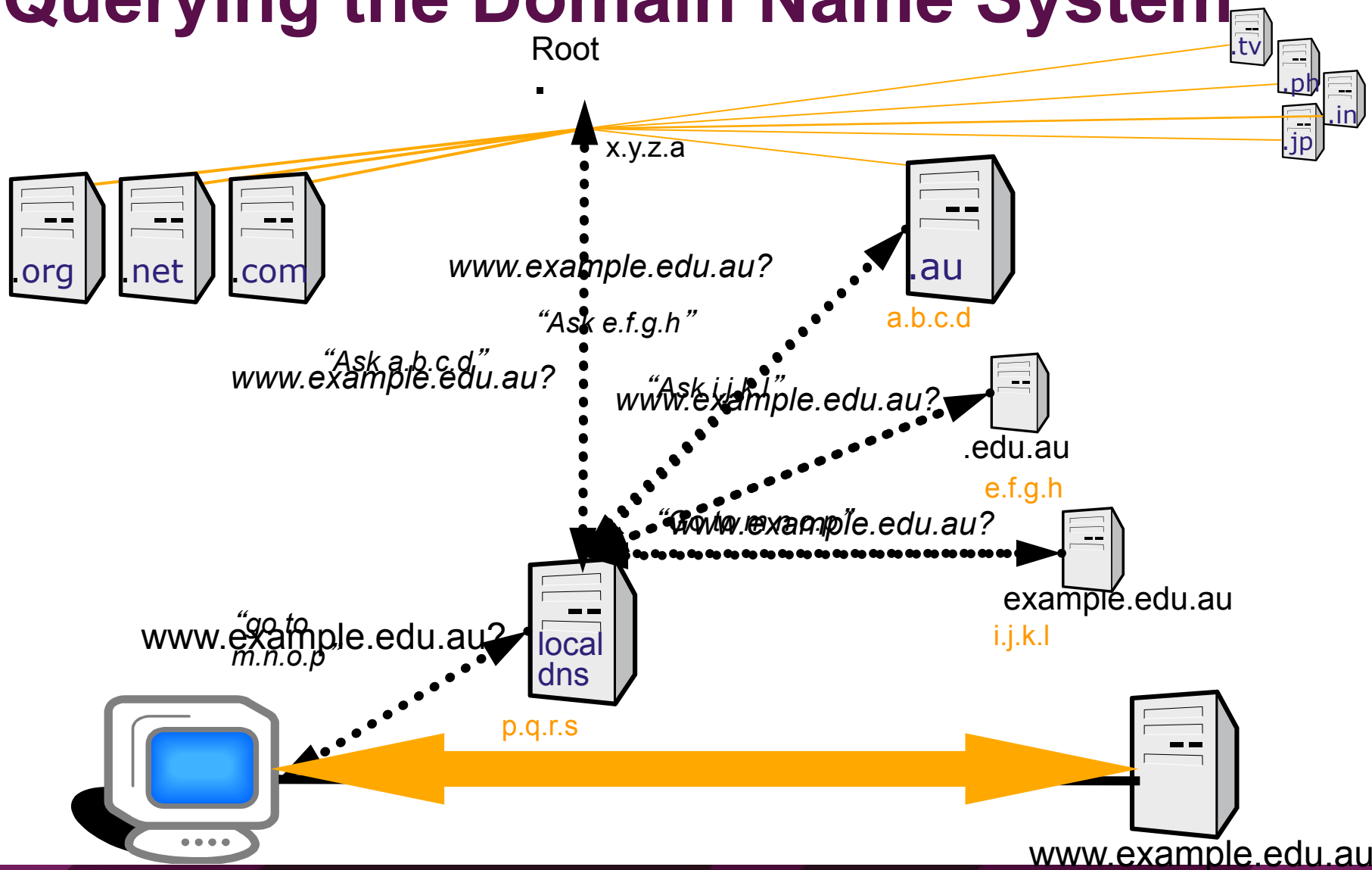
# Benefits of APNIC RR integrated in the whois

- Facilitates network troubleshooting
- Registration of routing policies
- Generation of router configurations
- Provides global view of routing

# Domain Name System Security Extensions (DNSSEC)

APNIC

# Querying the Domain Name System



# APNIC and reverse DNSSEC

- An attacker could intercept these DNS queries and return a corrupted response
- Protect against false DNS information to ensure you are communicating with the correct website or other service
- Browser can check to make sure the DNS information is not modified
- Works with other services like email (SMTP), instant messaging and VoIP
- APNIC is a link in the Chain of Trust for Reverse DNS

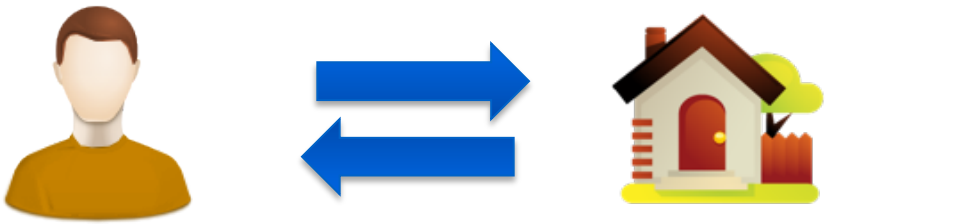
# Reverse DNS

APNIC

# APNIC also manages Reverse DNS

- ‘Forward DNS’ maps names to numbers
  – www.example.edu.au ➔192.168.28.131

- ‘Reverse DNS’ maps numbers to names
  – 202.12.28.131 ➔ www.example.edu.au



Person (Host)

Address (IPv4/IPv6)

# Reverse DNS

- Service denials
  - That only allow access when fully reverse delegated
- Diagnostics
  - Assisting in network troubleshooting
- Spam prevention
  - Reverse lookup to confirm the mail servers and source of the email
  - Failed lookup adds to an email's spam score
- Registration responsibilities

# Resource Public Key Infrastructure (RPKI)

APNIC

# What is RPKI?

- A robust security framework for verifying the association between resource holders and their Internet resources
  - Enables the creation and storage of digital certificates and associated Route Origin Authorization (ROA) documents
- Route Origin Authorizations (ROAs)
  - Certificate holder uses its private key to sign a ROA
  - Verifies that an AS has been given permission to advertise routes
- Prevents “route hijacking”
  - When an entity participating in Internet routing announces a prefix without authorization
  - Reason: malicious attack or operational mistake

# Route Origin Authorizations (ROAs)

- Certificate holder uses its private key to sign a ROA
- Verifies that an AS has been given permission by an address block holder to advertise routes to one or more prefixes within that block
- RPKI in the RIRs – Resource Certification
  - APNIC has implemented RPKI Resource Certification as an initiative to improve inter-domain routing and augmenting the information published in the whois database

# RPKI

- Working with ICANN and the other RIRs towards a global system
- Updated UI in MyAPNIC
- Ability for the public to run their own RPKI system interoperating with APNIC
- Public testbed is now live
  - Conducting interoperability testing with JPNIC, ARIN, LACNIC, and RIPE code
  - Chains of resources demonstrated from the other RIRs in both the ERX and transfer space

# “Right” to resources

- ISPs get their resources from the RIR
- ISPs notify its upstream of the prefixes to be announced
- Upstreams **must** check the whois database if resources have been delegated to a customer ISP

# Two components

- Certificate Authority (CA)
  - Internet Registries (RIR, NIR, Large LIR)
  - Issues certificates for customers
  - Allows customers to use the CA's GUI to issue ROAs for their prefixes
- Relying Party (RP)
  - Software which gathers data from CAs

# APNIC's role in stability and security

- LEA engagement plan
  - Training and Capacity building
  - Appointment of security specialist to assist
- APNIC Whois Database & Internet Routing Registry
  - Used to track down the source of network abuse
  - IP addresses, ASNs, reverse domains, routing policies
- Domain Name System Security Extensions (DNSSEC)
  - Reverse DNS only –suitable for email, VoIP, and other services
- Resource Certification
  - Verify the right to announce routes

# Thank you!

Adam Gosling

adam@apnic.net

@bout_policy