Driving the Future

Business case for IPV6 & DNSSEC

- shailesh.gupta@tatacommunications.com
There are different views about what makes a successful business. Typically success should be judged by the ability to meet objectives. Using this definition, success criteria would include:

- High levels of Sales
- High levels of Profits
- High levels of Consumer Satisfaction
- Production of high quality products
- Strong reputation
- Sustained growth

Businesses are able to establish targets in relation to each of the aspects of the bottom line e.g. increasing profit by x %, gaining employee satisfaction of y%, and minimizing their environmental impact. The success of businesses can then be judged in terms of their ability to meet important targets and creating a cycle of stakeholder satisfaction. Successful businesses take a long term rather than a short term view of success. Attaining success involves meeting objectives for a range of desirable outcomes, which create a cycle of stakeholder satisfaction.
IANA Unallocated Address Pool Exhaustion: 03-Feb-2011

Projected RIR Address Pool Exhaustion Dates:

- APNIC: 19-Apr-2011 (actual) 0.9091
- RIPE NCC: 14-Sep-2012 (actual) 0.9847
- ARIN: 21-Aug-2013 3.1782
- LACNIC: 31-May-2015 3.1733
- AFRINIC: 05-Nov-2019 4.1093
APNIC Survey in 2009 wrt IPV6 adoption

**APNIC Survey - 2009 (N=118)**

*Why not considering IPV6*

- Don’t see business need: 58%
- Communications Sp: 42%
- Haven’t gotten around do it: 33%
- Lack of config Meta tool: 23%
- ISP does not support IPV6: 19%
- Our Infra does not support: 18%
- Can’t afford expense: 14%
- Can’t afford risk of transition: 14%

*Source – APNIC Survey report*
Policy decisions taken by Governments

- 2008 **US** federal agencies IPv6 compliant
- 2010 25% of **EU** traffic to be over IPv6
- 2011 **JP** Govt target to have all JP ISPs over IPv6
- 2012 **AU** Govt networks over IPv6

“National IPv6 Deployment Roadmap” was released by the Government of India in **July 2010**:

- All major Service providers (having at least 10,000 internet customers or STM-1 bandwidth) will target to handle IPv6 traffic and offer IPv6 services by **December-2011**
- All central and State government ministries and departments, including its PSUs, shall start using IPv6 services by **March-2012**
- Formation of the IPv6 Task Force with one Oversight Committee, one Steering Committee and 10 working groups.
Only 18.5 million IPv4 addresses for a population of 1.2 billion in India.

- But the requirement for IP addresses will keep increasing with new services, new networks, new applications.

- Telecommunications will be largest consumer of IP addresses in coming years (Broadband, 3G, NGN, 4G, LTE etc.).

- IPv4 is a diminishing resource and is very costly @ USD 10 per IPV4 compared to IPv6 (almost free) right now and will be more costlier with passage of time.

It's not only about benefits from IPV6 but loosing the opportunities by not adopting it.

*IPv6 is the only solution!*
Data flow through the DNS

Where are the vulnerable points?

DNS Known Threats (RFC 3833)
- Packet Interception - man-in-the-middle attacks
- ID Guessing and Query Prediction
- Name Chaining - Cache Poisoning
- Betrayal By Trusted Server
- Denial of Service
- Wildcards

Registrar & Registrants

Server vulnerability

Registrar & Registrants

Man in the Middle

primary DNS

Secondary DNS

spoofing & Man in the Middle

Registry

© Copyright 2012 Tata Communications Ltd. All rights reserved.
There are 13 name servers associated with the root level; they are called \textit{root servers}. Two of the root servers are currently run by the U.S private-sector corporation VeriSign; the rest are operated by other organizations around the world as a service to the Internet community. The organizations that run name servers associated with a TLD are called \textit{registries}. Generally, ccTLDs are run by designated registries in the respective countries, and gTLDs are run by global registries. For example, VeriSign currently manages the name servers for the .com and .net TLDs, a nonprofit entity called Public Internet Registry (PIR) manages the name servers for the .org TLD, and another nonprofit organization called EDUCAUSE manages the name servers for the .edu TLD.
Before security objectives can be determined, the building blocks of the DNS need to be specified. DNS includes the following entities:

- **DNS hosting environment**
  - Host platform (O/S, file system, communication stack)
  - DNS software (name server, resolver)
  - DNS data (zone file, configuration file)

- **DNS transactions**
  - DNS query/response
  - Zone transfers
  - Dynamic updates
  - DNS NOTIFY

- **Security administration**
  - Choice of algorithms and key sizes (TSIG and DNSSEC)
  - Key management (generation, storage, and usage)
  - Public key publishing and setting up trust anchors
  - Key rollovers (scheduled and emergency)

- Install a DNSSEC capable name server implementation.
- Check zone file(s) for any possible integrity errors.
- Generate asymmetric key pair for each zone and include them in the zone file.
- Sign the zone. Load the signed zone onto the server.
- Configure name server to turn on DNSSEC processing.
DNSSEC provides message authentication and integrity verification through cryptographic signatures. Before a DNSSEC signed zone can be deployed, a name server must be configured to enable DNSSEC processing. In BIND, it is done by adding the following line to the options statement in the named configuration file (named.conf).

```plaintext
options {
  dnssec-enable yes;
};
```

After restart, the name server will now perform DNSSEC processing for DNS Query/response transactions.

### DNSSEC features
* End-to-end data integrity check.
* DNS data origin authentication.
* Authenticated denial of existence.

### Digital Signature Algorithms, Min. Key Sizes, and Crypto Periods

<table>
<thead>
<tr>
<th>Key Type</th>
<th>Digital Signature Algorithm Suite</th>
<th>Key Size</th>
<th>Crypto Period (Rollover Period)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key-Signing Key (KSK)</td>
<td>RSA-SHA1 (RSA-SHA-256) until 2015</td>
<td>2048 bits</td>
<td>12-24 months (1-2 years)</td>
</tr>
<tr>
<td>Zone-Signing Key (ZSK)</td>
<td>RSA-SHA1 (RSA-SHA-256) until 2015</td>
<td>1024 bits</td>
<td>1-3 months (30-90 days)</td>
</tr>
</tbody>
</table>

### DNS Transaction Threats and Security Objectives

<table>
<thead>
<tr>
<th>DNS Transaction</th>
<th>Threats</th>
<th>Security Objectives</th>
<th>IETF Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Query/Response</td>
<td>(a) Forged or bogus response</td>
<td>(a) Data origin authentication</td>
<td>DNSSEC</td>
</tr>
<tr>
<td></td>
<td>(b) Removal of records (RRs) in responses</td>
<td>(b) Data integrity verification</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(c) Incorrect application of wildcard expansion rules</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zone Transfer</td>
<td>(a) Denial of service</td>
<td>(a) Mutual authentication</td>
<td>TSIG</td>
</tr>
<tr>
<td></td>
<td>(b) Tampering of messages</td>
<td>(b) Data integrity verification</td>
<td></td>
</tr>
<tr>
<td>Dynamic Update</td>
<td>(a) Unauthorized Updates</td>
<td>(a) Mutual authentication</td>
<td>TSIG, GSS-TSIG or SIG(0)</td>
</tr>
<tr>
<td></td>
<td>(b) Tampering of messages</td>
<td>(b) Data integrity verification</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(c) Replay attack</td>
<td>(c) Signed timestamps</td>
<td></td>
</tr>
<tr>
<td>DNS NOTIFY</td>
<td>(a) Spurious notifications</td>
<td>(a) To prevent denial of service through</td>
<td>Specify hosts from</td>
</tr>
<tr>
<td></td>
<td></td>
<td>increase in workload</td>
<td>which this message</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>can be received</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>TSIG or SIG(0)</td>
</tr>
</tbody>
</table>
Business case for DNSSEC

Making a business case for DNSSEC is not easy in comparison to IPV6. DNSSEC is important - securing the DNS is a good thing - *Is this enough?*

Reducing the effort…

• This means bring down the cost of implementing DNSSEC
  – Research & Share
  – Simplify
  – Automate
  – Reduce risk

Examples:

• Registrars – Toolkits
• Registrants – One click DNSSEC
• ISPs – Simple DNSSEC resolvers
• End Users – Build it into software and turn on by default
Business case for DNSSEC

Make DNSSEC a requirement:

– Contractual obligation
– Government mandate like IPV6
– ICANN

Potential reason for deploying DNSSEC:

- Increased Security
– Really will only work if visible to end users
– Think green-bar in a browser
– Requires education

Secure DNS as an enabler

-DNS is now 100% trust worthy, what can we do with that?
-If what I can do is worthy, I will NEED DNSSEC
Business Benefits & Motivation for DNSSEC roles

Early adopters lead the pack

Cost drivers

- Infrastructure cost
- Strategic positioning

Registry (Responsible for tech operation of TLDs, manage registration within TLD)

- Become a reliable Trust Anchor
- Lead by example and stimulate parties further down in the chain to adopt DNSSEC
- Earn recognition in the DNS community

Zone operator (Responsible for tech operation of DNS zones & domain names)

- Provide assurance to clients that domain name services are reliable and trustworthy
- Look forward to increasing adoption rate when revenue is an important driver.
- Deploying DNSSEC can be profitable

Registrar (Accredited by ICANN to manage the reservation of domains as per policy)

- Differentiator and competitive advantage versus others

Recursive Resolver Operator (ISPs)

- Assure end-users on DNS reliability and trustworthiness
- Offering differentiator and competitive advantage
Thank You